



OneTouch™ AT G2 and OneTouch™ AT Network Assistant

User Manual

Revised 01/2018 for Software Release v6.5.1
© 2018 NETSCOUT SYSTEMS, Inc. All Rights Reserved.
All product names are trademarks of their respective companies.

LEGAL NOTIFICATION

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

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

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

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

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

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

Contents

Chapter 1: Get Acquainted

Overview of Features	1
Safety Information	3
Contact NETSCOUT	6
Additional Resources	6
AC Adapter and Battery	6
Charge the Battery	6
Switch the Power On	7
Set the Language	7
Check the Battery Status	7
Extend Battery Operating Time	7
Extend the Life of the Battery	8
Install and Use the Strap	9
OneTouch Platform	9
Remove and Install a Module	10
Connectors, Keys, and LEDs	11
Port A and Port B Connectors	15
Receive (Rx)/Link and Transmit (Tx) LEDs	17
The HOME Screen	19
Shortcut Bar	20
Test Tiers	21
Touchscreen	24
Entering Text	24
Entering Passwords and Other Hidden Text	25
URL Keyboard	26
IPv4 Address Entry Keyboard	27
IPv6 Address Entry Keyboard	28
Set Preferences	29
Language	29
Date/Time	29
Number Format	30
Units for Length Measurements	30
Timeout Periods (Power-Down and Backlight)	30

Power Line Frequency 30

Chapter 2: Setup Wizard

Setup Wizard 33
Working with the Setup Wizard 33
 To Start the Setup Wizard at a Later Time 33
Connect to the Management Port 34
 Handling Management Port Connection Problems 34
Setting up the Cloud Service 36
Configuring the Analyzer's Settings and Tests 36
 Setup Wizard Completion 41

Chapter 3: Basic Operation

Adding User Tests 43
 Add a TCP Test to the Home Screen 43
Connect to a Network 47
 Establish a Wired (Copper) Connection 47
 Establish a Fiber Connection 48
 Establish a Wi-Fi Connection 48
Run AutoTest 52
 Icons Indicate Test Status 53
View the Test Results 54
 View Detailed Test Results 55
Add More User Tests 56
Organize User Tests on the Test Tiers 57
Rename the Clouds 57
See Off-Screen Tests 58
Run a Single User Test Again 58
Edit a User Test 58
Move, Copy, or Delete a User Test 59
More About AutoTest 59
Next Steps 60
 View Other Test Results 60
 Run Path Analysis, Browse to, or Telnet/SSH to a Test's
 Target Server 60
 Configure the OneTouch Analyzer to Use SNMP . 61

Store Your Test Setup in a Profile	61
See Wi-Fi Analysis	61
See IPv6 Results	61
Generate a Report	62
Set Up Remote Control of the Analyzer	62

Chapter 4: Network Infrastructure Tests

OneTouch Instrument	63
Cable Test	69
Copper Cable Test	69
Fiber Cable Diagnostics	74
Link Test	75
PoE Test	76
Wi-Fi Analysis	82
Nearest Switch Test	82
Wi-Fi Network Connect Test	86
Gateway Test	92
DHCP Server Test	95
DNS Server Test	99
Wired Analysis	102

Chapter 5: User Tests

To Add a User Test	103
To Edit a User Test	104
Ping (ICMP) Test	105
Purpose	105
Configuration	105
How it Works	106
Results	107
Connect (TCP) Test	109
Purpose	109
Configuration	109
Results	112
Web (HTTP) Test	114
Purpose	114
Configuration	114

- How it Works 116
- Results 116
- File (FTP) Test 119
 - Purpose 119
 - Configuration 119
 - How it Works 121
 - Results 122
- Email (SMTP) Test 124
 - Purpose 124
 - Configuration 124
 - How it Works 125
 - Results 126
- Wired Performance Test 129
 - Purpose 129
 - Configuration 130
 - Run the Test 139
 - How it Works 139
 - Results 139
- Wi-Fi Performance Test 144
 - Purpose 144
 - Configuration 145
 - Run the Test 149
 - How it Works 149
 - Results 150
- Multicast (IGMP) Test 154
 - Purpose 154
 - Configuration 154
 - How it Works 155
 - Results 155
- Video (RTSP) Test 156
 - Purpose 156
 - Configuration 157
 - How it Works 157
 - Results 158

Chapter 6: Profiles

- Asterisk (*) After the Profile Name 162

Open the Profiles Screen	162
Save a Profile	162
Load a Profile	163
Rename or Delete a Profile	163
Export and Import Profiles	163
View a Profile File	165
Editing Profiles	165

Chapter 7: Wired Analysis

Wired Analysis	167
Description	167
Configuration	168
SNMP	169
Slow Discovery	169
How Wired Analysis Works	169
Results	170
To Show Wired Device Details	173
Wired Analysis Tools	177
Add Test	177
Port Scan	178
Path Analysis	179
MultiPort Statistics	184
Web Browser	190
Telnet/SSH	190

Chapter 8: Wi-Fi Analysis

OneTouch AT G2 Additional Wi-Fi Features	193
Enable Wi-Fi	193
Enable Connect Mode	194
Wi-Fi Icon on the HOME Screen	194
Stopped	194
Linked and testing	195
Linked but not actively testing	195
Scanning	195
Wi-Fi Analysis	196
Passive Wi-Fi Analysis	196

- Active Wi-Fi Analysis 196
- Wi-Fi Analysis Screens 196
- Network Analysis 197
 - To Show Network Details 200
 - Network Details 202
- Access Point Analysis 203
 - To Show AP Details 206
 - AP Details 207
- Client Analysis 213
 - To Show Client Details 216
 - Probing Client Details 221
- Channel Analysis 222
 - Channel Overview 225
 - To Show Channel Details 226
- Interferer Analysis 228
 - To Show Interferer Details 231
- Wi-Fi TOOLS 234
 - Name Tool 234
 - Authorization Status Tool and Default Setting .. 235
 - Connect Tool 238
 - Locate Tool 243

Chapter 9: Tools

- Test Settings 248
 - Wired 248
 - Wi-Fi 252
 - Analysis 253
- Link-Live Cloud Tools 253
 - Claim Unit: 253
 - Cloud Proxy: 254
 - Port: 254
 - Upload AutoTest Results: 254
 - Periodic AutoTest 254
 - Cloud Remote: 255
 - Unit Name: 255
- Testing Tools 256
 - Capture 256

VoIP Analysis	256
Wi-Fi Network Validation	268
iPerf Test	280
Performance Peer	292
Browser	292
Telnet/SSH	294
Toner	294
Flash Port	295
FiberInspector/WebCam	295
WebCam and Remote View	298
File Tools	299
Profiles	299
AP Authorization	299
Reports	300
Screens	306
Maintenance Tools	307
Version Information	307
Management Port	308
Battery Status	312
Language	312
Date/Time	312
Number	312
Length	312
Timeout Period	313
Audible Tone	313
Power Line Frequency	313
Display	313
Update Software	314
Options	315
Export Logs	315
Factory Defaults (Erase Data)	316

Chapter 10: Packet Capture

General Information about Capture Filters	319
Filters Perform a Logical AND Operation	320
Packet Capture Speed and Dropped Frames	321
SD Card	321

- Wired Packet Capture Connection Options 321
 - Port A Only (Single-ended Packet Capture) 321
 - Ports A and B 322
 - Inline Packet Capture 322
- To Configure Wired Packet Capture 323
- Port A Filter and Port B Filter 324
 - MAC 324
 - VLAN 324
 - IP 324
 - Port 324
 - NOT 324
 - IPv6 324
 - COPY FROM B and COPY FROM A Buttons 325
- Speed/Duplex 325
- File Size Limit and Frame Slice Size 325
 - Frame Size Limit 325
 - Frame Slice Size 325
- Next Step 325
- Wi-Fi Packet Capture 325
 - Enable Wi-Fi 326
- Configure Wi-Fi Packet Filtering 327
- To Manually Configure a Filter 327
 - Channel 328
 - Channel Mode 328
 - Device BSSID/MAC 329
 - Control Frames 329
 - Data Frames 329
 - Management Frames 330
 - Files Size Limit and Frame Slice Size 330
 - File Format 330
- Next Step 330
- To Automatically Configure a Filter 331
- Open the Wi-Fi ANALYSIS Screen 331
 - Filter by AP 331
 - Filter by Client 333
 - Filter by Channel 334
- Start Packet Capture 334
- Stop Packet Capture 336
- AutoTest Capture 337

To Enable or Disable AutoTest Capture	337
To Save an AutoTest Capture	337
Managing Capture Files	338
Analyzing Capture Files	339

Chapter 11: Managing Files

Using the Built-in File Manager	341
Remote User Interface and File Access	347
User Interface Remote Control	348
Remote File Access	349
Other Remote Access Information	352
SD Card	353
USB Flash Drive	353

Chapter 12: Maintenance

Maintenance	355
Clean the Analyzer	355
Extend the Life of the Battery	355
Store the Analyzer	356
Remove and Install the Battery	356

Chapter 13: Link-Live Cloud Service

Overview	359
Link-Live Cloud Service Support Page	359
Infrastructure and User Tests in the Cloud	359
Setting Up and Accessing the Cloud Service	360
Creating a Link-Live.com Account	360
Claiming Your Unit	360
Setting up Periodic AutoTest	361
Naming your OneTouch AT	364
Remote Access from the Cloud	365
Preparing Your Unit for Remote Access	365

Chapter 14: Specifications

Environmental and Regulatory Specifications	367
Cables	368
Network Ports	368
Supported Network Standards	368
SFP Adapters	369
Wi-Fi Antennas	369
Wi-Fi Adapter	369
Power	372
Certifications and Compliance	372
Memory	373
Headset Jack	373
Dimensions	373
Weight	373
Display	373
Regulatory Information	373
FCC and IC Interference Statement	374
Identification Numbers	375
Exposure to RF Energy	376
Regulatory Statements	378

List of Figures

1	The OneTouch AT Network Assistant.....	2
2	Install and Use the Hang Strap	9
3	Remove and Install a Module	10
4	Features of the Main Unit	11
5	Left Side View	12
6	Right Side View.....	13
7	Insert the SD Card	14
8	Top End View - Connectors.....	15
9	Top End View - LEDs	16
10	Battery Compartment.....	18
11	Kensington Security Slot	18
12	The OneTouch AT Home Screen	19
13	Keyboards for Text Entry.....	25
14	Keyboard for URL Entry.....	26
15	Keyboard for IPv4 Address Entry	27
16	Keyboard for IPv6 Address Entry	28
17	Management Port Button in TOOLS Menu.....	35
18	Management Port IP Address	35
19	The Home Screen	44
20	ADD TEST Screen.....	45
21	Connect (TCP) Test Setup Screen	45
22	URL Keyboard	46
23	Wi-Fi Test Settings Screen	49
24	Signal Offsets Screen with Channel Selected.....	51
25	Noise Offsets Screen with Bands Selected.....	52
26	HOME Screen After Running AutoTest	54
27	Connect (TCP) Test Results Tab	55
28	Seeing Off-Screen Tests	58
29	Wired OneTouch Results	65
30	Wi-Fi OneTouch Results.....	68
31	Cable Connected to WireMapper #1	71
32	Shielded Crossover Cable Connected to WireMapper #1.....	71
33	Unterminated Cable Connected to Port A	72
34	Unterminated Cable with Shorts and Opens	72
35	Cable Connected from Port A to Port B	73
36	Cable With Only Two Pairs of Conductors	73
37	No Cable Connected	74

OneTouch AT and OneTouch AT G2

User Manual

38	Fiber Cable Shown on HOME Screen	74
39	HOME Screen - PoE Test Passed	78
40	Detailed PoE Test Results - Test Passed.....	79
41	HOME Screen - PoE Test Failed	80
42	Detailed PoE Test Results - Test Failed.....	81
43	Nearest Switch - PORT Tab	84
44	Nearest Switch - STATISTICS Tab	85
45	Wi-Fi Network Connect Test Results.....	88
46	Roaming Navigation Controls	91
47	Gateway WIRED Tab	94
48	Gateway Wi-Fi Tab	95
49	DHCP Test Results.....	97
50	DHCP Path Analysis	99
51	DNS Test Results	101
52	Add Test Screen.....	103
53	Ping Test Results.....	107
54	TCP Test Results.....	112
55	Web (HTTP) Test Results	117
56	FTP Test Results	122
57	Email (SMTP) Test Results	126
58	Email Sent From IPv4 Wired Connection	128
59	Email Sent From IPv4 Wi-Fi Connection.....	128
60	Wired Performance Test - Performance Peer Screen	132
61	Wired Performance Test Setup Tab	137
62	Wired Performance Test Results Using a Single Frame Size	140
63	Test Results: RFC 2544 Sweep, Tabular View.....	141
64	Test Results: RFC 2544 Sweep, Graphical View	142
65	Wi-Fi Performance Setup Tab.....	146
66	Wi-Fi Performance Test Results.....	151
67	Multicast (IGMP) Test Results	155
68	Video (RTSP) Test Results.....	158
69	WIRED ANALYSIS Setup Screen.....	168
70	WIRED ANALYSIS Screen	170
71	Displaying Wired Device Details	173
72	Wired Device Details.....	174
73	Port Scan Results	179
74	Wired Analysis Tools Menu	181
75	Path Analysis Results.....	182
76	Path Analysis - Detailed Results	184
77	MultiPort Statistics Button on Wired Analysis Tools Menu	185
78	MultiPort Statistics Button on Path Analysis Tools Menu	186
79	MultiPort Statistics Summary Screen	187

80	MultiPort Statistics Details Screen	189
81	MultiPort - Device on Port Details Screen	190
82	Wi-Fi Analysis Tabs.....	197
83	Wi-Fi Network Analysis Tab, Sorted by SSID	198
84	Displaying Wi-Fi Network Details	201
85	Wi-Fi Network Details.....	202
86	AP Analysis Tab	204
87	AP Details	208
88	Bonded Channel AP Details	211
89	Client Analysis Tab.....	214
90	Associated Client Details	217
91	Probing Client Detail	221
92	Channel Analysis Tab.....	223
93	Channel Overview.....	225
94	Wi-Fi Channel Details	226
95	Interferer Analysis Tab	229
96	Interferer Details.....	232
97	Wi-Fi AP Tools Screen	234
98	AP Authorization Status.....	238
99	Multiple Choices for Connect tool.....	239
100	Network (left) and AP (right) Connect Tool Results	240
101	Network (left) and AP (right) Connection Logs	242
102	Directional Antenna Holder.....	244
103	AP/Client LOCATE Screen	245
104	Interferer LOCATE Screen.....	246
105	Tools Screen	247
106	Link-Live Cloud Tools.....	253
107	Testing Tools	256
108	The VoIP Analysis Configuration Screen, SETUP Tab.....	258
109	The VoIP Analysis Results Screen, MONITOR Tab	259
110	The VoIP Analysis Results Screen, LOG Tab	261
111	The VoIP Analysis Configuration Screen	263
112	The VoIP Analysis - Save VoIP Capture	264
113	The Wi-Fi Network Validation Screen	269
114	Wi-Fi Network Validation SSID Selection Screen	270
115	Manage Locations for Wi-Fi Network Validation	271
116	Discovered BSSIDs for Wi-Fi Network Validation.....	272
117	Wi-Fi Network Validation in Progress	274
118	Wi-Fi Network Validation Results Tab.....	275
119	iPerf Test Setup Screen	281
120	iPerf Server Screen	282
121	UDP Protocol Parameters	284

OneTouch AT and OneTouch AT G2
User Manual

122	Select BSSIDs for iPerf Test	285
123	Wired iPerf TCP Test Results	286
124	Wired iPerf UDP Test Results	287
125	Wi-Fi iPerf UDP Test Results	289
126	FiberInspector Image of an Endface	296
127	FiberInspector Image with Measurement Scales.....	297
128	File Tools.....	299
129	Initial Available Report Options.....	300
130	Save Report Screen—Possible Report Options.....	302
131	Report Content Options for AutoTest	303
132	Report Content Options for Wired Analysis.....	304
133	Report Content Options for Wi-Fi Analysis	305
134	Maintenance Tools.....	307
135	Management Port Screen Linked Wired	309
136	Battery Status Screen	312
137	Capture Filters - Logical AND Operation	320
138	Single-Ended Packet Capture	321
139	Inline Packet Capture.....	322
140	The Wired CAPTURE Screen	323
141	Wi-Fi Test Settings Screen.....	326
142	Wi-Fi CAPTURE SETTINGS Screen	328
143	Wi-Fi CAPTURE Screen	332
144	CAPTURE SETTINGS Screen	333
145	Wired Capture Results	335
146	Wi-Fi Capture Results.....	336
147	The Four File Manager Screens	343
148	SAVE AS Screen	344
149	Manage Profiles Screen	345
150	File Manager - Export File Tree	346
151	Browser Remote Access Login Credentials	348
152	Remote Access OneTouch Home Screen.....	349
153	OneTouch Web Server Home	350
154	OneTouch Remote File Access.....	350
155	Remote Access icon located in Shortcut Bar	352
156	Management Port Status Dialog - Remote Control Disconnect..	353
157	Remove and Install the Battery.....	357
158	Periodic AutoTest Status Screen.....	363

Chapter 1: Get Acquainted

Overview of Features

The OneTouch™ AT Network Assistant is a rugged, easy to use, hand-held 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/ac Wi-Fi interface
- Network services measurements
- USB Type A port

OneTouch AT and OneTouch AT G2 User Manual

- 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 and optional USB Wi-Fi management port adapter
- Ethernet packet capture and Wi-Fi packet capture

The analyzer features a Setup Wizard that guides you through configuring the analyzer for testing. See “Setup Wizard” on [page 33](#).








Figure 1. The OneTouch AT Network Assistant

Safety Information

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

Table 1. Symbols

	Warning or Caution: Risk of damage or destruction to equipment or software. See explanations in the manuals.
	Warning: Risk of fire, electric shock, or personal injury.
	Warning: Class 1 laser when an SFP module is installed. Risk of eye damage from hazardous radiation.
	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

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

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

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

 **Warning: Class 1 and Class 2 Laser Products** 

To Prevent eye damage and personal injury:

- Do not look directly into optical connectors. Some optical equipment emits invisible radiation that can cause permanent damage to your eyes.

- Do not look into the laser. Do not point laser directly at persons or animals or indirectly off reflective surfaces.
- When you inspect fiber endfaces, use only magnification devices that have the correct filters.
- Use the Product only as specified or hazardous laser radiation exposure can occur.

 **Caution**

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

Contact NETSCOUT

For more contact information, go to our website.



<http://enterprise.netscout.com>



customercare@netscout.com



Toll free: +1-844-833-3713

International: 978-320-2150

Additional Resources

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

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

AC Adapter and Battery

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

Charge the Battery

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


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

Notes



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

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


Switch the Power On

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


Set the Language

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

Check the Battery Status

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

When the AC adapter is connected to the analyzer, the AC Power Indicator LED (see Figure 5) is red while the battery is charging; green when fully charged. If the battery's temperature is too high or too low to permit charging, the AC Power Indicator turns yellow.

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

Extend Battery Operating Time

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

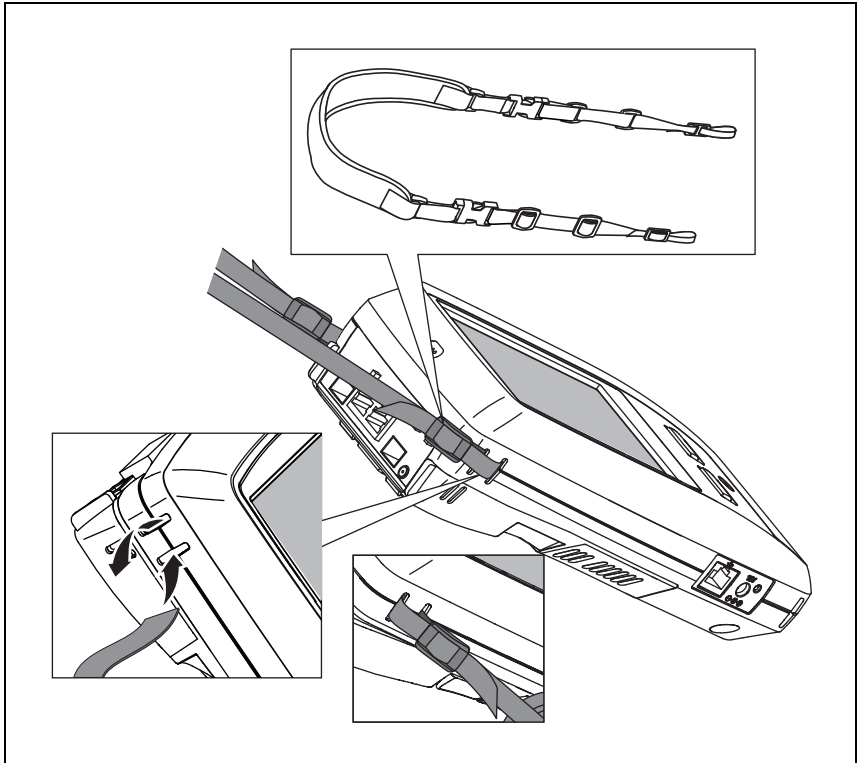
You can make the backlight shut off after a period of inactivity. You can also make the analyzer power down after a period of inactivity. See "Timeout Periods (Power-Down and Backlight)" on [page 30](#).

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.



GV0013.EPS

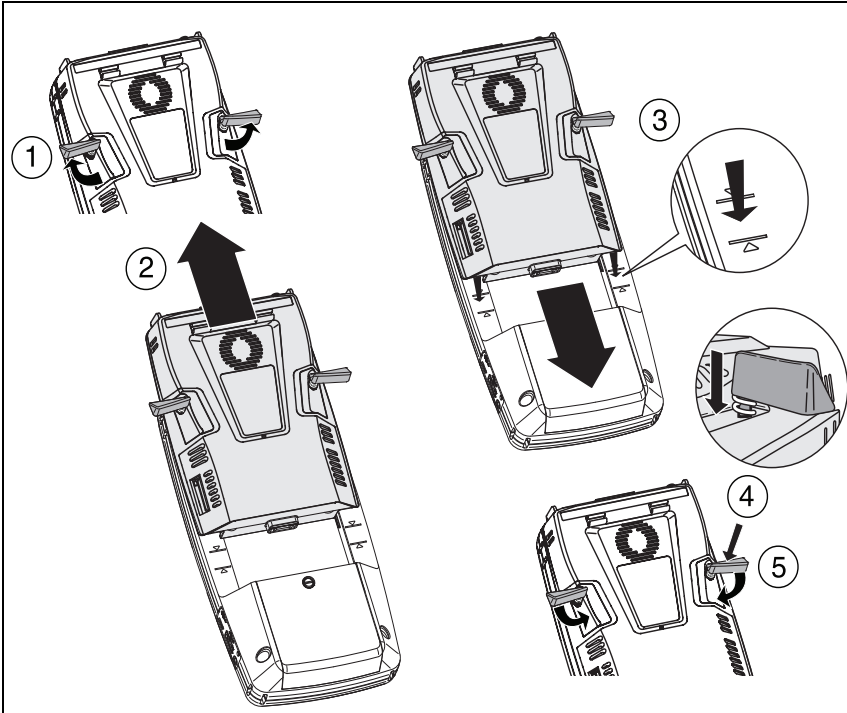
Figure 2. Install and Use the Hang Strap

OneTouch Platform

The OneTouch platform is a handheld computer and display platform that accepts modules like the OneTouch AT G2 module. The modules attach to the system as shown.

Remove and Install a Module

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

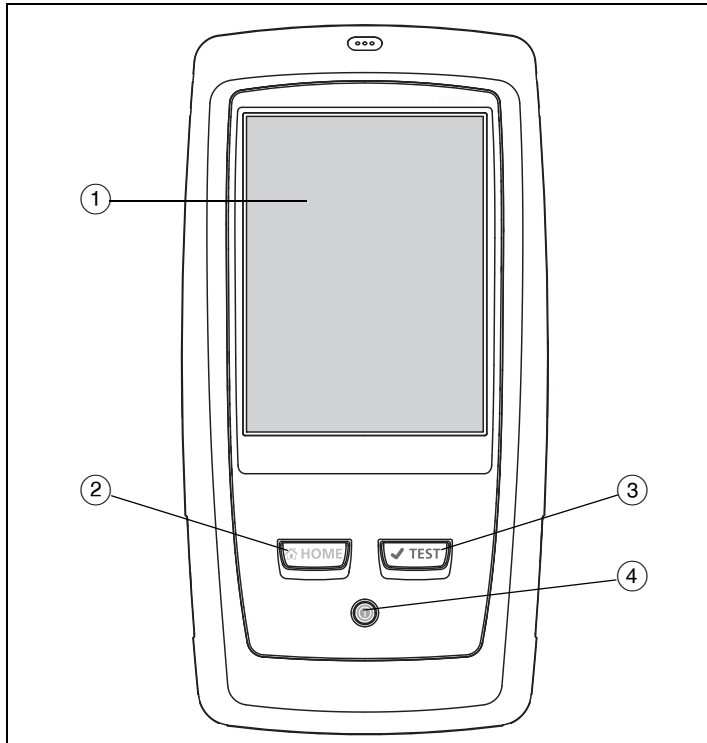


GVO004.EPS

Figure 3. Remove and Install a Module

Connectors, Keys, and LEDs



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

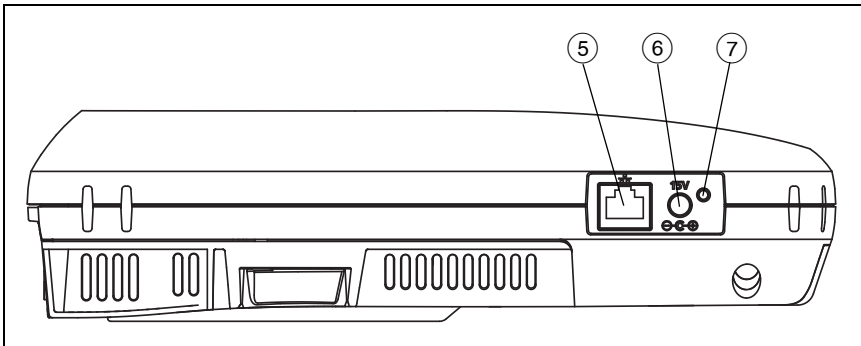


GVO005.EPS

Figure 4. Features of the Main Unit

- ① **LCD display with touch-screen** - To change the brightness, tap **TOOLS > Display**. See also: "Touchscreen" on [page 24](#).
- ② **HOME** - Press this key to go to the Home screen. See "The HOME Screen" on [page 19](#).

- ③ **AutoTest key**  - 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  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 6](#).

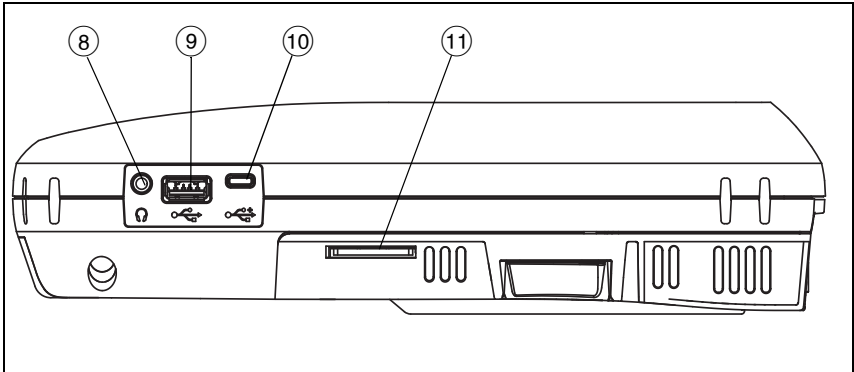


GVO006.EPS

Figure 5. 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 6](#).
- ⑦ **AC Power Indicator** - This LED is red while the battery is charging; green when fully charged.



GV0007.EPS

Figure 6. Right Side View

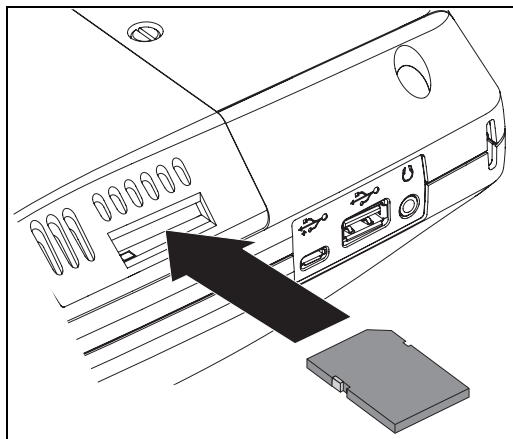
- ⑧ **Headphone Jack** - This 3.5 mm connector is provided so you can use headphones when using the Wi-Fi locate feature.
- ⑨ **USB-A Connector** - This connector is for the Wi-Fi Management Port feature and for managing files on a USB storage device such as a flash drive. See Chapter 11: "Managing Files," beginning on [page 341](#).

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.

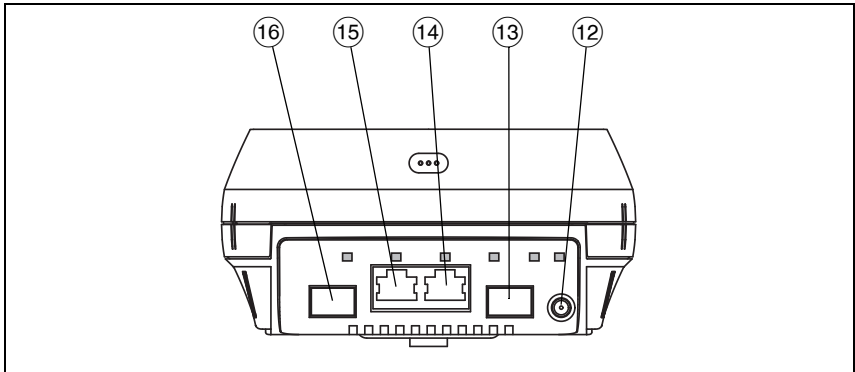
- ⑪ **SD Card Slot** - This is for inserting an SD card. You can manage files on an SD card. See Chapter 11: "Managing Files," beginning on [page 341](#).



GVO015.EPS

Figure 7. 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.



GVO008.EPS

Figure 8. Top End View - Connectors

- ⑫ External Antenna Connector (see “Connect Tool” on [page 238](#))
- 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)

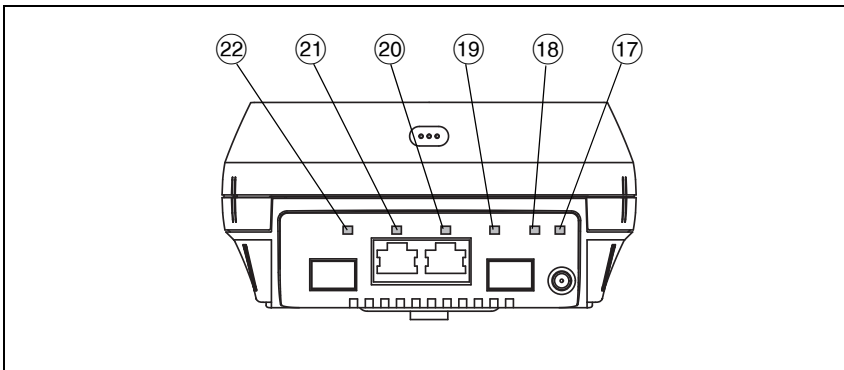
To connect to a network using a copper cable, make a connection to the Port A RJ45 jack. Appropriate cable and fiber types are listed in Chapter 14: “Specifications,” beginning on [page 367](#).

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  or press the AutoTest  key.

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



GVO008.EPS

Figure 9. Top End View - LEDs

- ①⑦ Wi-Fi Link/Scanning/Monitoring LED
- ①⑧ Wi-Fi Activity LED
- ①⑨ Port A Link LED
- ①⑩ Port A Activity LED
- ①⑪ Port B Link LED
- ①⑫ Port B Activity LED

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

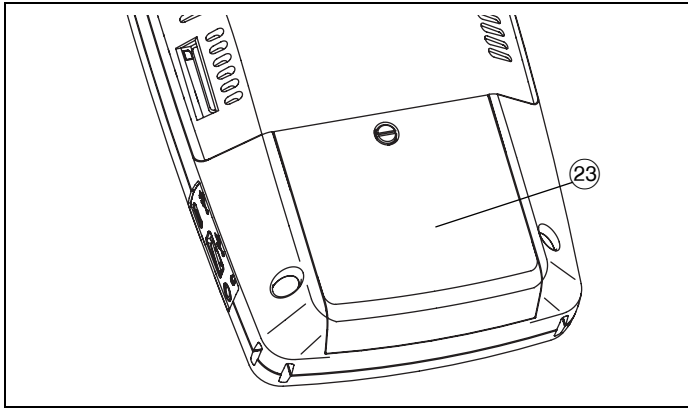
The Management Port and each Ethernet port (Port A, Port B, and Wi-Fi) have two LEDs: “Link” and “Activity.”

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

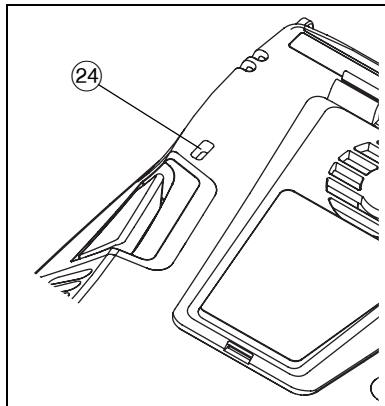
LED State	Meaning
Off	No activity
Flashing Green	Receive or transmit activity



GVO012.EPS

Figure 10. Battery Compartment

- ②③ Battery Compartment - The battery pack can be replaced. See “Remove and Install the Battery” on [page 356](#).




GVO016.EPS

Figure 11. 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.

The HOME Screen

Press the  key to display the Home screen.

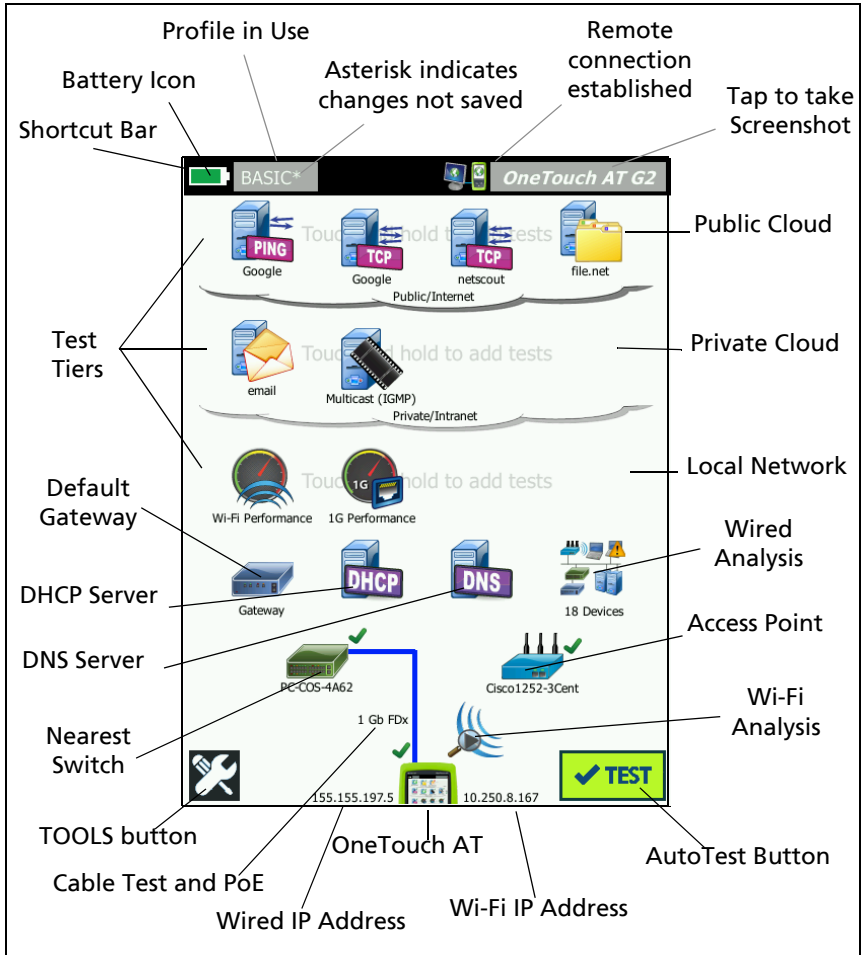


Figure 12. The OneTouch AT Home Screen


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.

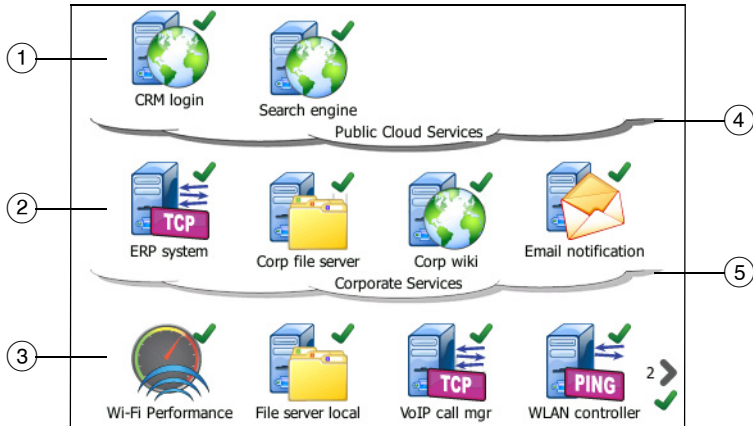
Test warnings (indicated by a warning icon ⚠ next to a test's icon on the HOME screen) do not affect the pass/fail status of AutoTest.

- 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 6](#).

- 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 "Asterisk (*) After the Profile Name" on [page 162](#).
- 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 306](#), "Reports" on [page 300](#), and "To Save an AutoTest Capture" on [page 337](#).

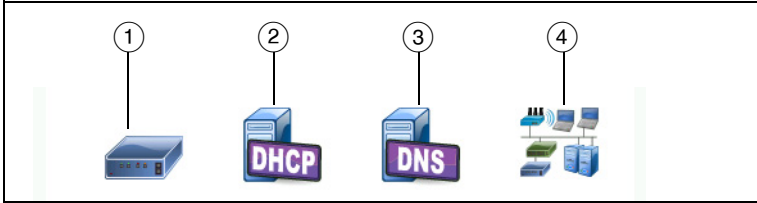
Test Tiers



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

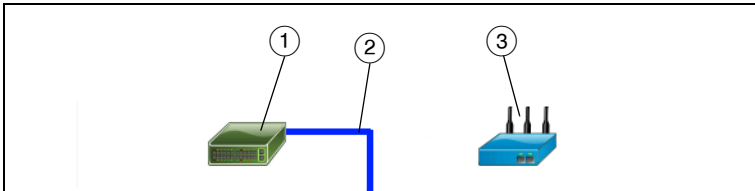
- ① **Public Cloud Tier:** This tier is generally used for tests of servers that are in the public cloud (the internet).
- ② **Private Cloud Tier:** This tier is generally used for tests of servers that are in the private cloud (the corporate intranet).
- ③ **Local Network Tier:** This tier is generally 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 57](#).
- ⑤ **Private/Intranet Cloud:** Touch the cloud to rename it. See [page 57](#).

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 92](#).
- 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 95](#).
- 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 99](#).
- 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 167](#).

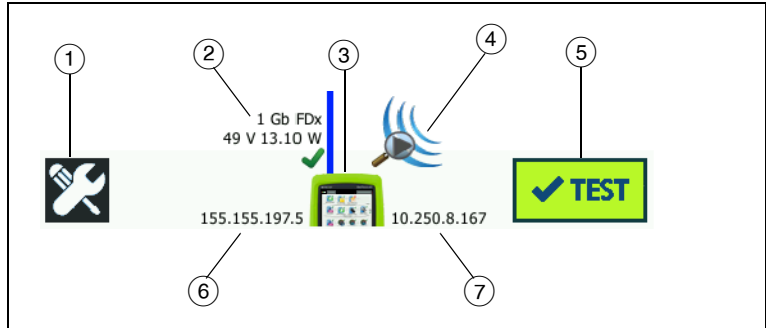
Network Access Tier




- 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 82](#).
- ② **Cable:** Tap the link icon to view cable and PoE statistics. See “Cable Test” on [page 69](#) and “PoE Test” on [page 76](#) 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 86](#).

Instrument Tier



- ① **TOOLS button:** Tap this button to enter the TOOLS menu. See Chapter 9: "Tools," beginning on [page 247](#).
- ② **Cable:** Tap the text to view cable, link, and PoE test results. See “Cable Test” on [page 69](#) and “PoE Test” on [page 76](#) 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.
- ④ **Wi-Fi Analysis:** Tap the icon to open the Wi-Fi Analysis screen. See Chapter 8: "Wi-Fi Analysis," beginning on [page 193](#).
- 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 ).
- 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.

Touchscreen

Caution

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

You can use these gestures on the touchscreen:

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

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

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

Entering Text

When you tap a panel to enter text, a keyboard is displayed on the bottom half of the screen (Figure 13).

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

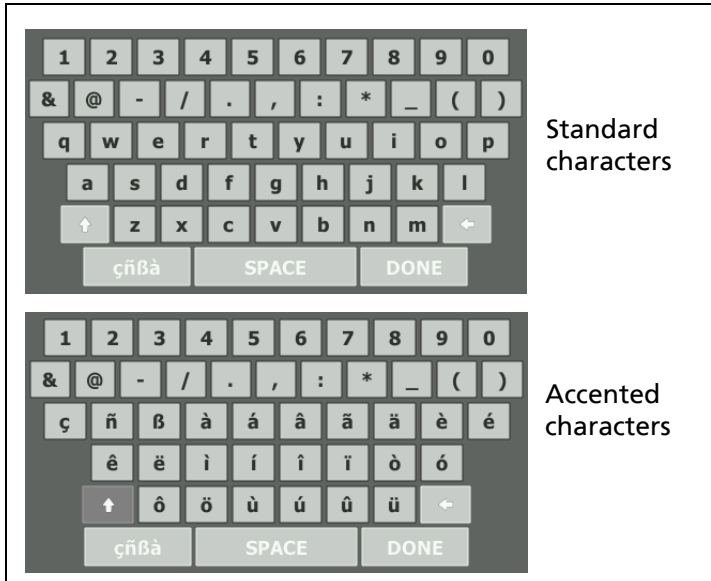


Figure 13. Keyboards for Text Entry

Entering Passwords and Other Hidden Text

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



To show characters in plain text as you type them:

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

- 3 Enter the characters



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

URL Keyboard

When entering a URL, the keyboard includes buttons for adding "www." to the beginning, or ".com," ".net," or ".org" to the end. See Figure 14.



Figure 14. 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 15.



Figure 15. Keyboard for IPv4 Address Entry

IPv6 Address Entry Keyboard

When entering an IPv6 address, the keyboard is customized with buttons for common number combinations, the colon separator, and hexadecimal digits. An IPv6 address is represented by 8 groups of 16-bit hexadecimal values separated by colons. Leading zeros can be omitted. Groups of consecutive zeros can be replaced by a double colon (::).



Figure 16. 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 7](#).

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 29](#).
 - 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: Setup Wizard



Before you use the analyzer, read the safety information that starts on page 3.

This chapter helps you quickly begin using the OneTouch analyzer.


Setup Wizard


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


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

Working with the Setup Wizard

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

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

- Keep the default selection (**Yes**), and tap the **NEXT** button  to complete the section.
- Select **No** and tap the **NEXT** button to skip the section.


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

To Start the Setup Wizard at a Later Time

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

- 1 Tap the **TOOLS** icon  on the HOME screen.
- 2 Tap the **Setup Wizard** button.

Connect to the Management Port

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


Handling Management Port Connection Problems

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

Proxy Server

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

Ensure that the management port received an IP address

- 1 Exit the Setup Wizard.
- 2 Tap the **TOOLS** icon  on the HOME screen.

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

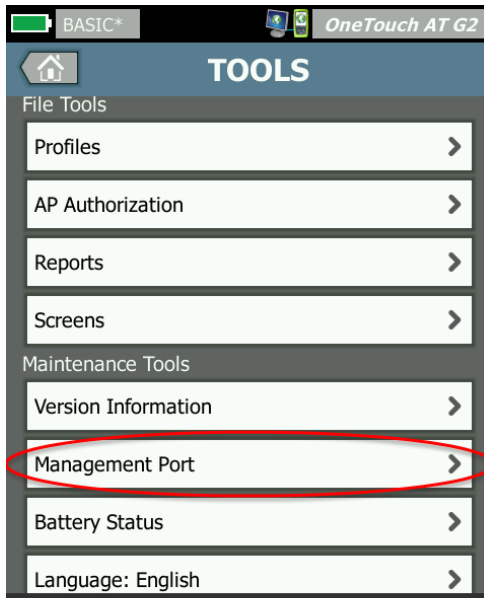


Figure 17. Management Port Button in TOOLS Menu


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



Figure 18. Management Port IP Address

If a static IP address is required

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

- 1 From the HOME screen, tap the TOOLS icon .
- 2 Scroll down to the Maintenance Tools section, and tap the **Management Port** button.
- 3 Tap the **Wired** button.
- 4 Tap **STATIC** on the **Address** button and set the address.

Setting up the Cloud Service

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

Follow the on-screen prompts.

For more information, see the following sections:

- "Working with the Setup Wizard" on [page 33](#)
- "Setting Up and Accessing the Cloud Service" on [page 360](#)
- "Handling Management Port Connection Problems" on [page 34](#)

Configuring the Analyzer's Settings and Tests

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

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

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

You can create multiple Profiles for performing specific sets of tests. For example, you may want to create Profiles to test

connectivity and performance for specific buildings on a site, specific departments within a business, or specific clients.

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

- Wired network settings
- Wi-Fi network settings
- SNMP configuration (Analysis)


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

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

The last sections of the Setup Wizard let you set up network connectivity, infrastructure/network services, network performance, and application and protocol performance tests. These are referred to as User Tests, and they are shown as icons on the Test Tiers (see [page 21](#)) on the HOME screen.

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

The entire configuration is stored in a Profile that you can easily recall and use. See Chapter 6: "Profiles," beginning on [page 161](#).


You can exit the Setup Wizard at any time before saving a Profile by selecting the EXIT button . Partially completed Profiles are not saved. You can re-start the Setup Wizard later, as described on [page 33](#).

Network Connectivity - Wired

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

For more information about wired network configuration, see “Analysis” on [page 253](#).


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

- 1 Tap **TOOLS**  at the bottom left corner of the HOME screen.
- 2 Select **Wired** from the list.

Network Connectivity - Wi-Fi

In the next section, you can configure your Wi-Fi network settings, e.g. RF bands, SSID security, and network address. For information about W-Fi network configuration, see “Establish a Wi-Fi Connection” on [page 48](#).

To manually configure Wi-Fi settings without using the Setup Wizard:

- 1 Tap **TOOLS**  at the bottom left corner of the HOME screen.
- 2 Select **Wi-Fi** from the list.


Infrastructure Analysis/Network Services

This portion of the Setup Wizard allows you to configure your network’s SNMP community strings to allow in-depth network analysis. For additional information about Network Analysis configuration, see “Analysis” on [page 253](#).

Note

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

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

- 1 Tap **TOOLS**  at the bottom left corner of the HOME screen.
- 2 Select **Analysis** from the list.



Network Performance

This Setup Wizard section lets you:

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

For information about the DHCP server test, see page 95, and for DNS test details, see page 99.

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

- 1 On the HOME screen, tap the **DHCP** icon  or the **DNS** icon .
- 2 Select the **SETUP** tab.

Application and Protocol Performance

This section of the Setup Wizard lets you add User Tests to the Profile. The list of User Tests is shown on [page 37](#). User Tests can verify performance of common applications and protocols running on your network.

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

For *detailed*, step-by-step instructions for adding a User Test without using the Setup Wizard, see "Adding User Tests" on [page 43](#).

For *general* instructions on adding user tests without using the Setup Wizard, see Chapter 5: "User Tests," beginning on [page 103](#).

Setup Wizard Completion

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

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

Chapter 3: Basic Operation



Before you use the analyzer, read the safety information that starts on page 3.

This chapter provides instructions for:

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

Adding User Tests

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

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

You can also add user tests from a Wired Analysis screen as described in “Wired Analysis Tools” on [page 177](#).

Add a TCP Test to the Home Screen

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

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

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

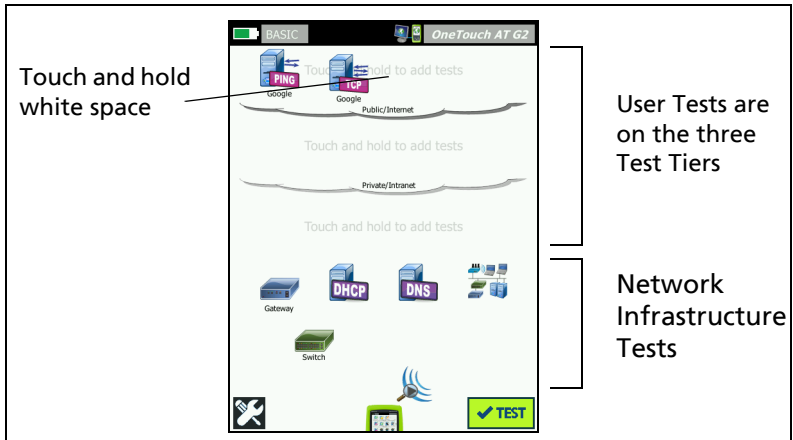


Figure 19. The Home Screen

The ADD TEST screen is displayed.

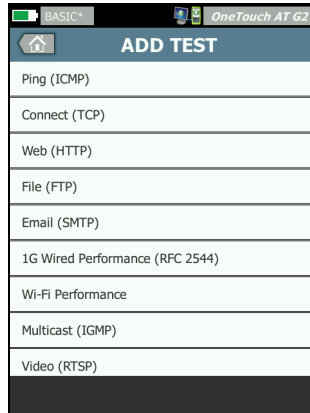


Figure 20. ADD TEST Screen

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

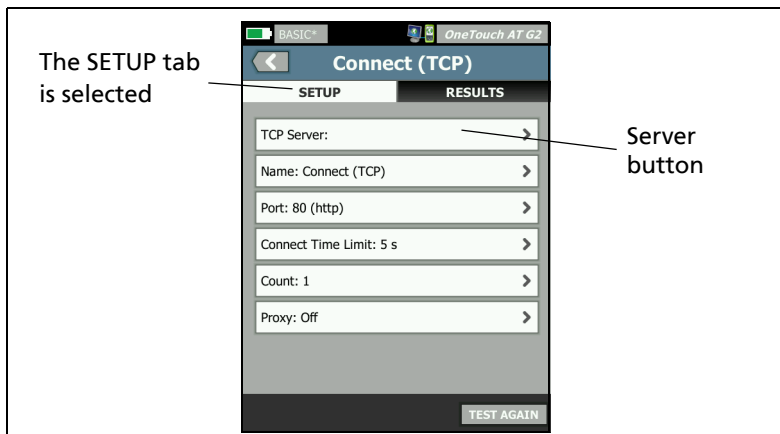



Figure 21. Connect (TCP) Test Setup Screen

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



Figure 22. URL Keyboard

- 4 At the top of the screen, tap the **URL** button.
 - The keyboard changes based on the type of information to be entered (e.g. IPv4 address, IPv6 address, URL).
 - Shortcut buttons (e.g. "www." and ".com") on the keyboard help you to enter information quickly and easily.
- 5 Tap the **www.** button.
- 6 Type **enterprise.netscout** using the keyboard keys.
- 7 Tap the **.com** button.
- 8 Tap the **DONE** button.
- 9 The **Name** button allows you to assign a custom name to a test. The test's name appears under the test's icon on the HOME screen and in OneTouch Reports. For your convenience, the OneTouch analyzer automatically names the test based on the URL or IP address. Tap the **Name** button if you want to change the name.

- 10 The **Port** button lets you specify the TCP port number on which the connection will be established. For this test do not change the port from the default, which is port 80 (HTTP).
- 11 The **Time Limit** button lets you choose the amount of time allowed for the test to complete. If the test doesn't complete in the allowed time, it will fail. Set the time limit to 10 seconds.
- 12 **Count** specifies the number of three-way handshakes that will be completed. Set **Count** to 1.
- 13 The **Proxy** control lets you specify a proxy server through which the TCP requests can be routed. If your network uses a proxy server, tap the **Proxy** button, tap **On**, and set the server's address and port. Otherwise, continue to the next step.
- 14 Press the  key to return to the HOME screen.

When you add a user test, an asterisk appears after the Profile name to indicate that it has been changed, but not yet saved. See also: Chapter 6: "Profiles," beginning on [page 161](#).

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 NETSCOUT. See [page 6](#) 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 scans for Wi-Fi networks, but it does not connect to any network until it is configured to do so.

To connect to a Wi-Fi network:

- 1 Press the  key on the front panel.
- 2 Tap the **TOOLS** icon .

- 3 Tap the **Wi-Fi** button under Test Settings.

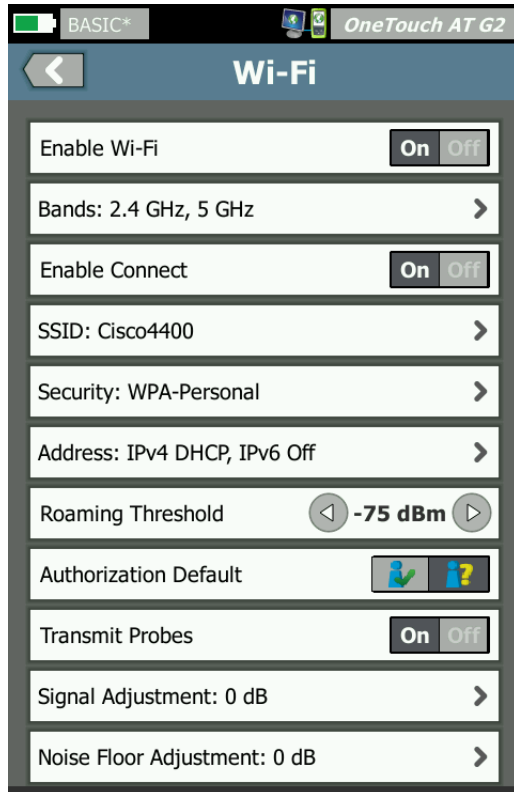



Figure 23. Wi-Fi Test Settings Screen

- 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 Set **Enable Connect** to **On**. When Enable Connect is set to **Off**, the OneTouch analyzer will perform Wi-Fi analysis (as described on [page 193](#)), but it will not connect to a Wi-Fi network.

- 7 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.
- 8 Tap the back button .
- 9 Tap the **Security** button and enter the selections that are appropriate for your network. TLS EAP types require a certificate for authentication. For more information on EAP security types and instructions for importing certificates, see [page 248](#). The process is the same for Wi-Fi and wired.
- 10 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.
- 11 *For OneTouch AT G2 only:* The **Roaming Threshold** determines the signal level at which the driver begins searching for an alternate access point with a better signal. Tap the left or right toggle buttons to adjust the threshold for your needs. The default is -75 dBm.
- 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 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 196](#).

- 14 The **Signal Adjustment** button allows you to customize the OneTouch analyzer signal level by channel to meet the testing needs of your specific Wi-Fi network and client environments. Tap the **Signal Adjustment** button to open the Signal Offsets screen.

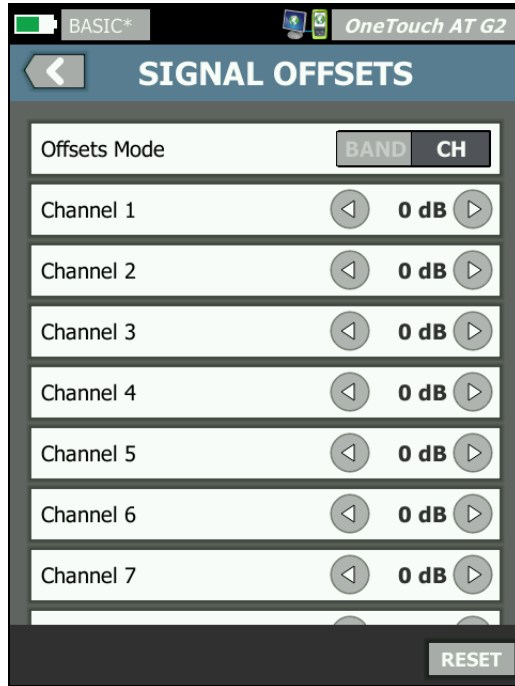



Figure 24. Signal Offsets Screen with Channel Selected

- 15 If you want to change the signal offsets, use the toggle button to select entire bands or individual channels to configure, and then use the arrow buttons to set the dB as needed.
- 16 Tap the back button .

- 17 The **Noise Floor Adjustment** button allows you to customize the OneTouch analyzer noise floor by channel to meet the testing needs of your specific Wi-Fi network and client environments. Tap the **Noise Floor Adjustment** button to open the Signal Offsets screen.

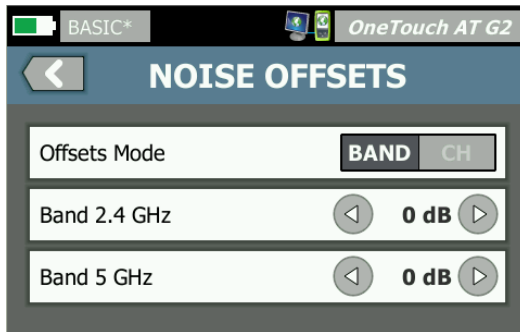






Figure 25. Noise Offsets Screen with Bands Selected

- 18 If you want to change the noise offsets, use the toggle button to select entire bands or individual channels to configure, and then use the arrow buttons to set the dB as needed.
- 19 Tap the back button .
- 20 Press the  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  (located at the lower-right corner of the HOME screen) or press the AutoTest key  (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 69](#))
- 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 337](#).

Icons Indicate Test Status

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

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



The test has not started. The icon is faded.





The test is in progress.



The test passed.





The test failed.

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

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

View the Test Results

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

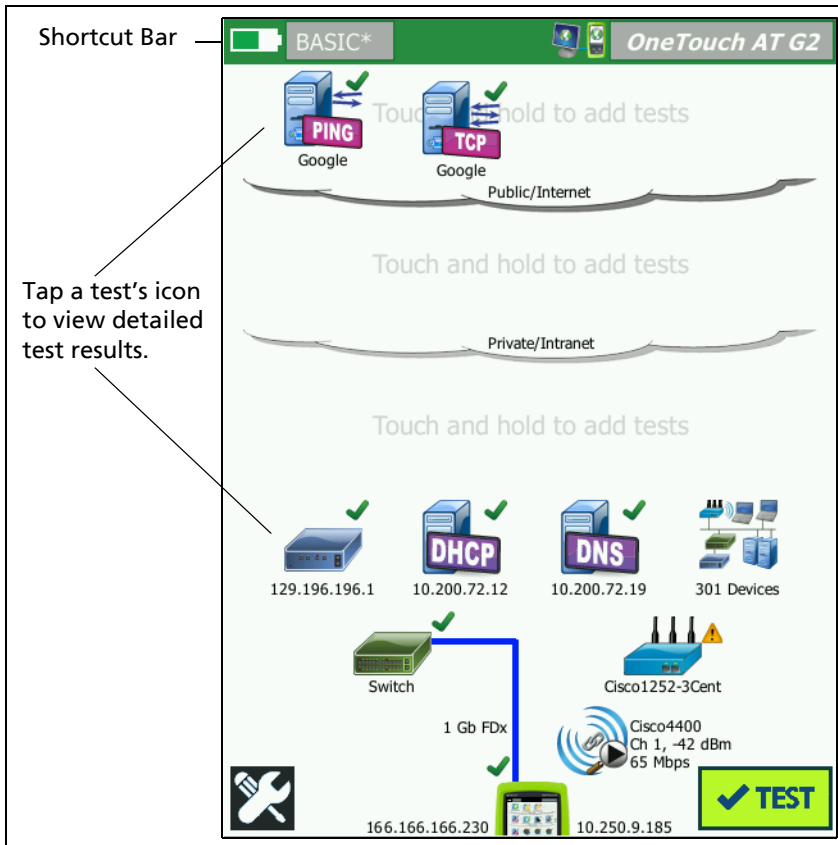


Figure 26. HOME Screen After Running AutoTest

View Detailed Test Results

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

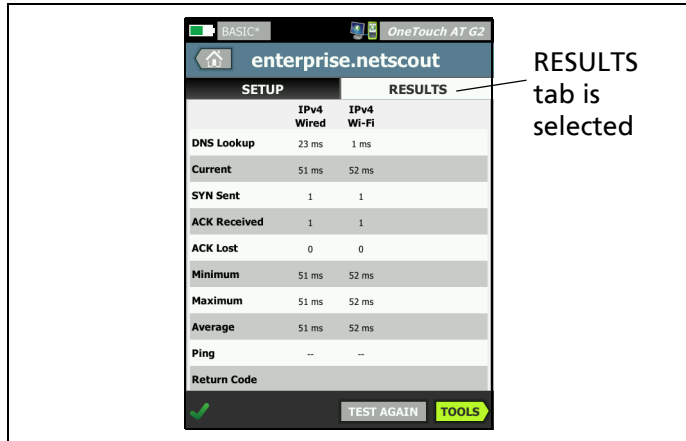


Figure 27. Connect (TCP) Test Results Tab

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 -- indicates 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  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  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 44](#).

You can also add user tests from a Wired Analysis screen as described in “Wired Analysis Tools” on [page 177](#).

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

- [Ping \(ICMP\) Test](#) (page 105)
- [Connect \(TCP\) Test](#) (page 109)
- [Web \(HTTP\) Test](#) (page 114)
- [File \(FTP\) Test](#) (page 119)
- [Email \(SMTP\) Test](#) (page 124)
- [Wired Performance Test](#) (page 129)
- [Wi-Fi Performance Test](#) (page 144)
- [Multicast \(IGMP\) Test](#) (page 154)
- [Video \(RTSP\) Test](#) (page 156)

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.

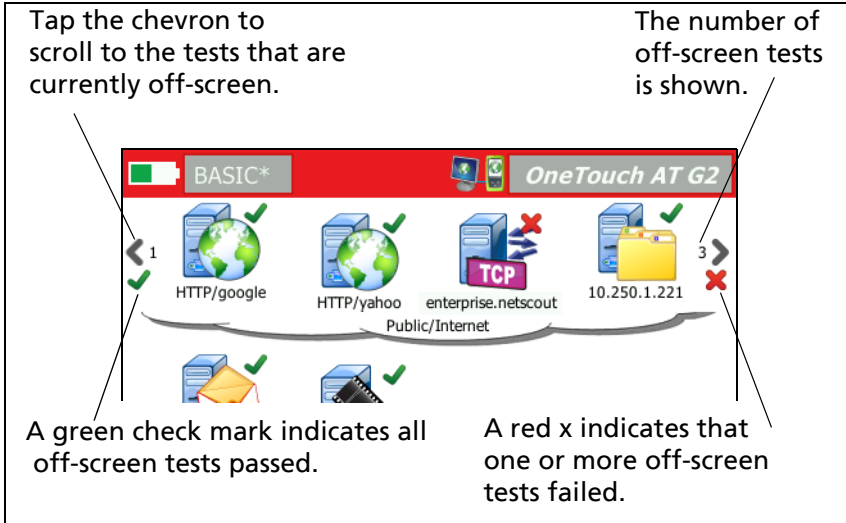



Figure 28. Seeing Off-Screen Tests

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 .

Edit a User Test

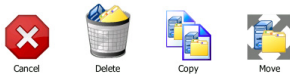
To edit a test, tap its icon. Tap the test's SETUP tab to edit the test parameters.

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

An asterisk is also displayed after the profile name at the top-left corner of the HOME screen, to indicate that the test profile has been changed. See Chapter 6: "Profiles," beginning on [page 161](#).

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 63](#).
- User Tests are described on [page 103](#).

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  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 179](#)

“Browse to a Test Target from the HOME Screen” on [page 293](#)

“Telnet/SSH” on [page 294](#)


Configure the OneTouch Analyzer to Use SNMP

Add SNMP Community Strings/Credentials to allow display of SNMP-enabled switch and gateway statistics, and enable cross-linking between wired and Wi-Fi device details via the Discovery Button. See “SNMP” on [page 169](#). See also: [page 173](#) and [page 211](#) 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 161](#).

See Wi-Fi Analysis

To see Wi-Fi analysis, tap the Wi-Fi analysis icon . See Chapter 8, “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 300](#).

Set Up Remote Control of the Analyzer

See “Remote User Interface and File Access” on [page 347](#).

Chapter 4: Network Infrastructure Tests

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

When the network infrastructure tests complete, your user tests will run. See “User Tests” on [page 103](#).

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

- [OneTouch Instrument, page 63](#)
- [Cable Test, page 69](#)
- [Link Test, page 75](#)
- [PoE Test, page 76](#)
- [Wi-Fi Analysis, page 82](#)
- [Nearest Switch Test, page 82](#)
- [Wi-Fi Network Connect Test, page 86](#)
- [Gateway Test, page 92](#)
- [DHCP Server Test, page 95](#)
- [DNS Server Test, page 99](#)
- [Wired Analysis, page 102](#)

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 47](#)) and tap the AutoTest button .

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  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



WIRED		Wi-Fi
Address		
IPv4	177.197.197.230	
Subnet	255.255.254.0	
IPv6 Link-Local	::	
IPv6 Global	::	
MAC Address	NetSct:00c017-c30000	
Management Port	197.197.197.0	
Unit Name	TW OneTouch	
Transmit Statistics		
Bytes	537,161	
Packets	4,717	

Figure 29. 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.

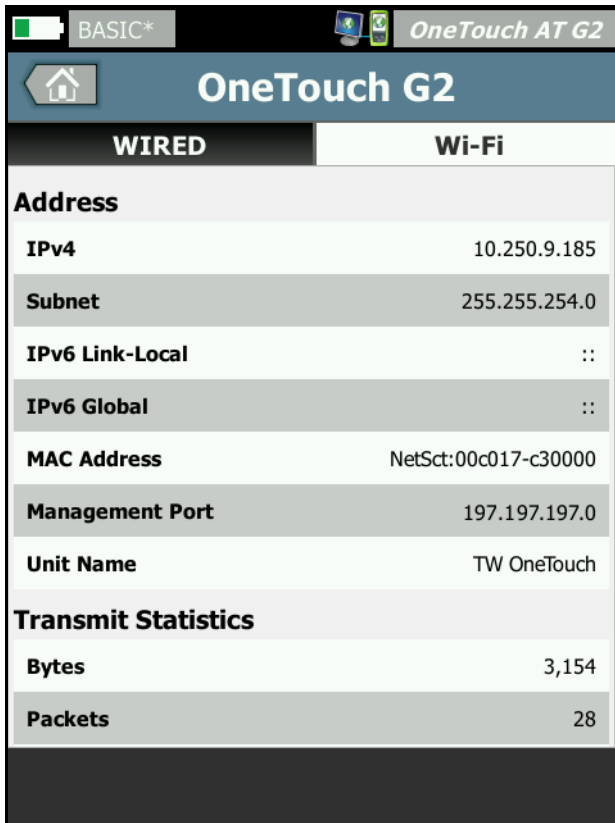
Alignment errors may manifest as an inability to connect to the network or as intermittent connectivity.

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.

Wi-Fi Results Tab



The screenshot shows the OneTouch G2 interface with the Wi-Fi tab selected. The top status bar includes a battery icon, the text 'BASIC*', signal strength icons, and the device name 'OneTouch AT G2'. Below this is a navigation bar with a home icon and the title 'OneTouch G2'. The main content area is divided into two tabs: 'WIRED' and 'Wi-Fi', with 'Wi-Fi' being the active tab. The data is organized into sections: 'Address' (IPv4, Subnet, IPv6 Link-Local, IPv6 Global, MAC Address, Management Port, Unit Name) and 'Transmit Statistics' (Bytes, Packets).

WIRED		Wi-Fi	
Address			
IPv4		10.250.9.185	
Subnet		255.255.254.0	
IPv6 Link-Local		::	
IPv6 Global		::	
MAC Address		NetSct:00c017-c30000	
Management Port		197.197.197.0	
Unit Name		TW OneTouch	
Transmit Statistics			
Bytes		3,154	
Packets		28	

Figure 30. Wi-Fi OneTouch Results


Figure 30 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



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 , 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 NETSCOUT 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
- Underterminated (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.

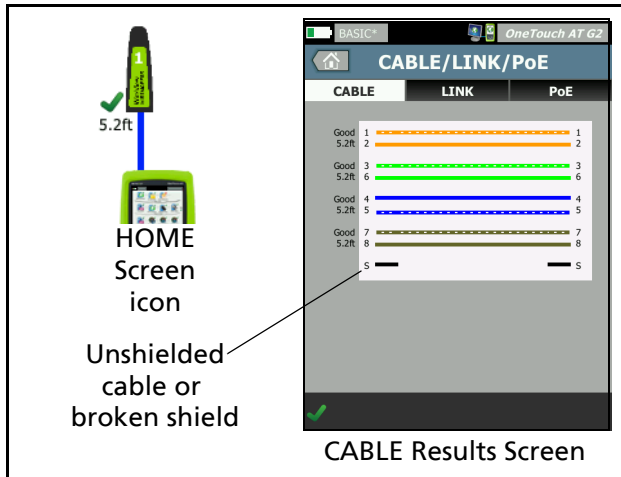


Figure 31. Cable Connected to WireMapper #1

This shows a cable connected to a 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.

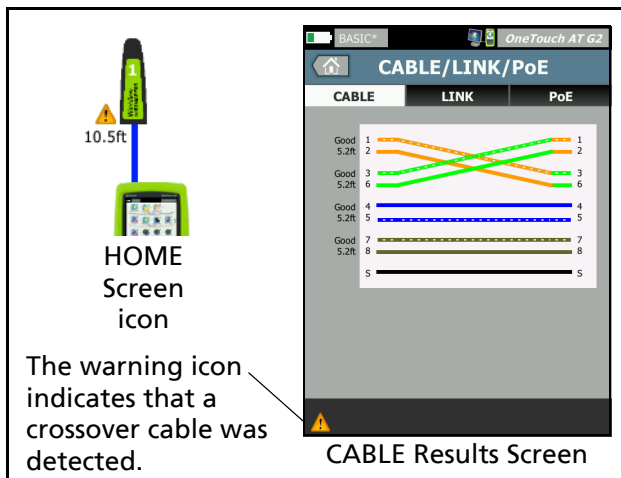


Figure 32. Shielded Crossover Cable Connected to WireMapper #1

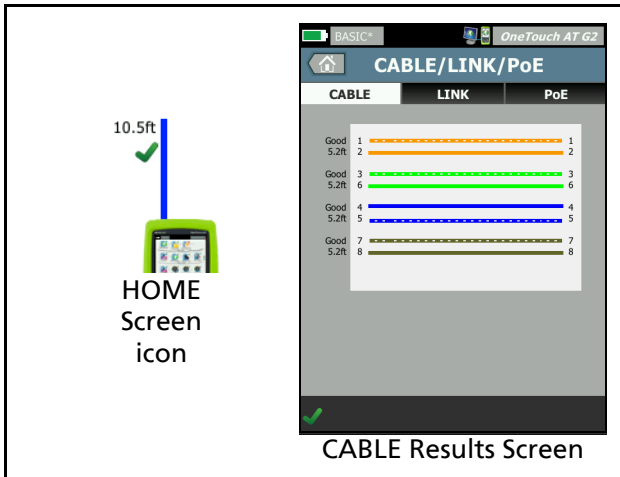
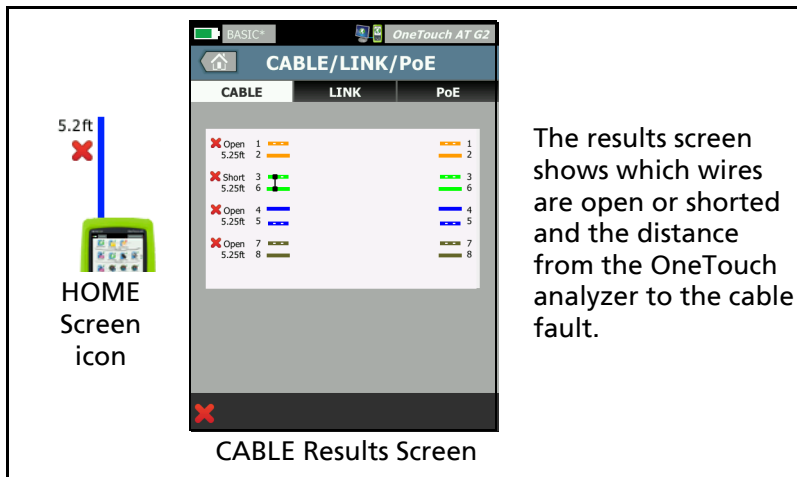


Figure 33. Underterminated Cable Connected to Port A



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

Figure 34. Underterminated Cable with Shorts and Opens

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

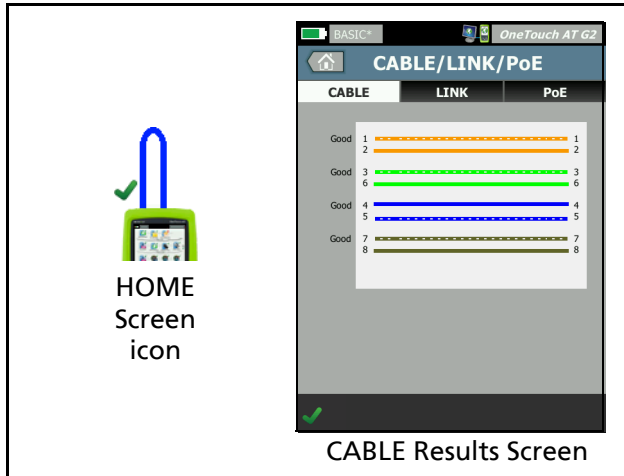


Figure 35. Cable Connected from Port A to Port B

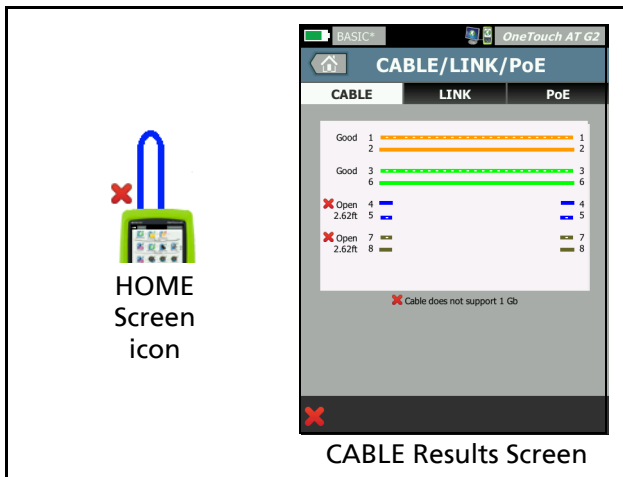


Figure 36. Cable With Only Two Pairs of Conductors

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

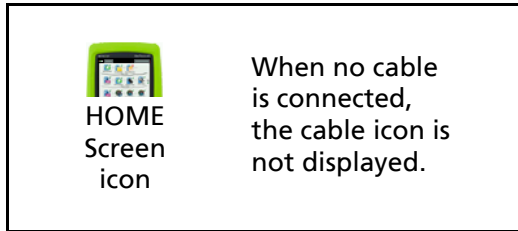


Figure 37. No Cable Connected

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.

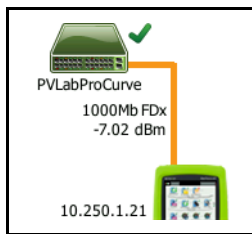


Figure 38. Fiber Cable Shown on HOME Screen

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  on the touchscreen or the AutoTest key  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.

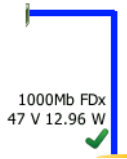
Rx Pair is the wire pair on which link negotiation was offered by the port.

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.

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

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  on the touchscreen or the AutoTest key  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.

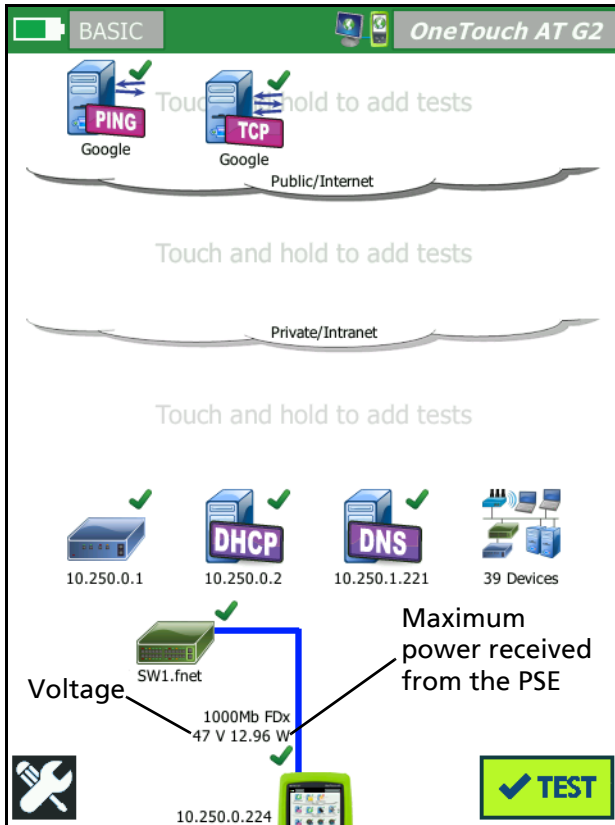


Figure 39. HOME Screen - PoE Test Passed

Figure 39 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.

CABLE	LINK	PoE
Requested Class		0 (13.00 W)
Received Class		0
PSE Type		1
Unloaded Voltage		51 V
Pairs Used		+:4,5 -:7,8
TruePower™ Voltage		49 V
TruePower™ Power		13.10 W

Figure 40. Detailed PoE Test Results - Test Passed

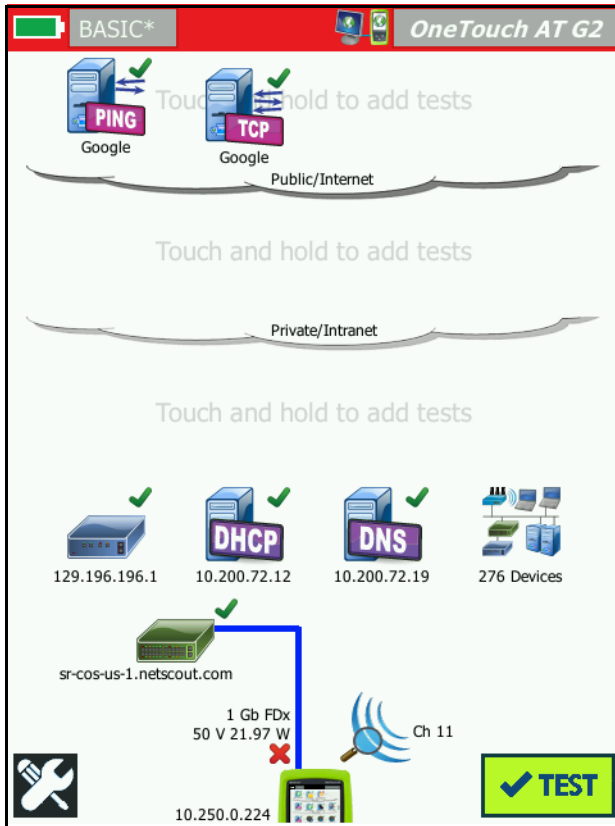


Figure 41. HOME Screen - PoE Test Failed


Figure 41 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 42 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.

CABLE	LINK	PoE
Requested Class		4 (25.50 W)
Received Class		✘ 0
PSE Type		1
Unloaded Voltage		49 V
Pairs Used		+:4,5 -:7,8
TruePower™ Voltage		50 V
TruePower™ Power		✘ 21.97 W

Figure 42. 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 8: "Wi-Fi Analysis," beginning on [page 193](#) 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 169](#).

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 Near-

est 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.

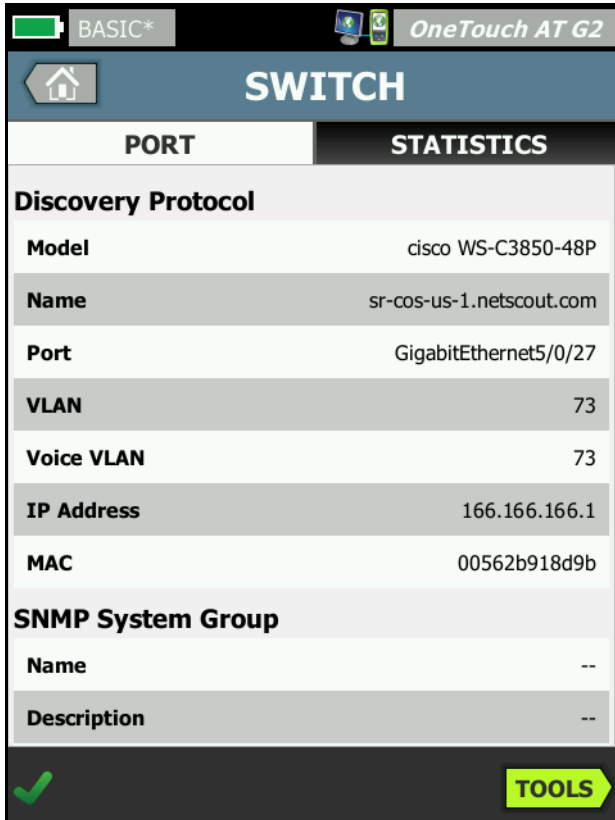




Figure 43. Nearest Switch - PORT Tab

PORT	STATISTICS	
	All Since 3:15 am	Last Sample 3:18:48 am
Receive Packets		
Unicasts	10,287	3
Multicasts	0	0
Broadcasts	676	0
Discards	0	0
Errors	0	0
Transmit Packets		
Unicasts	9,248	12
Multicasts	7,632	289
Broadcasts	14,687	1,390

Figure 44. Nearest Switch - STATISTICS Tab

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

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. 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 **Enable Connect** is **On**.
- 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 .

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 and view data for each AP the OneTouch connects to.

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

The navigation controls at the bottom of the RESULTS screen let you see connection results of previously roamed APs. If you are using a OneTouch AT G2, the reason for the roam is shown on the AP RESULTS tab, and the LOG tab displays the AP's roaming related scans and connections.

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 ✖ is shown next to the AP icon. The warning icon ⚠ is displayed if a warning condition occurred (see [page 89](#)), but the test otherwise passed. Tap the AP icon for detailed results.

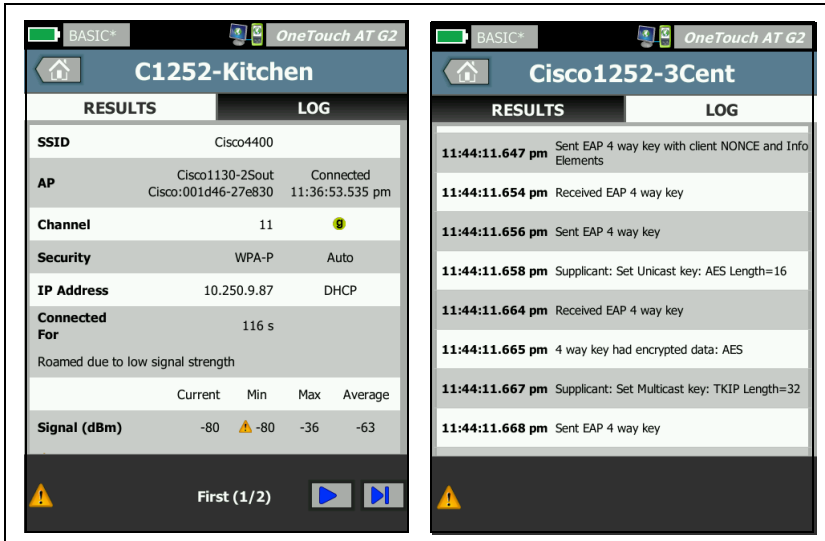


Figure 45. Wi-Fi Network Connect Test Results

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 48](#).

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.


For OneTouch AT G2 users: If you roam from one AP and connect to another AP, the reason for the roam appears here, under **Connected for**.


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. (See Figure 45.)


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.

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.

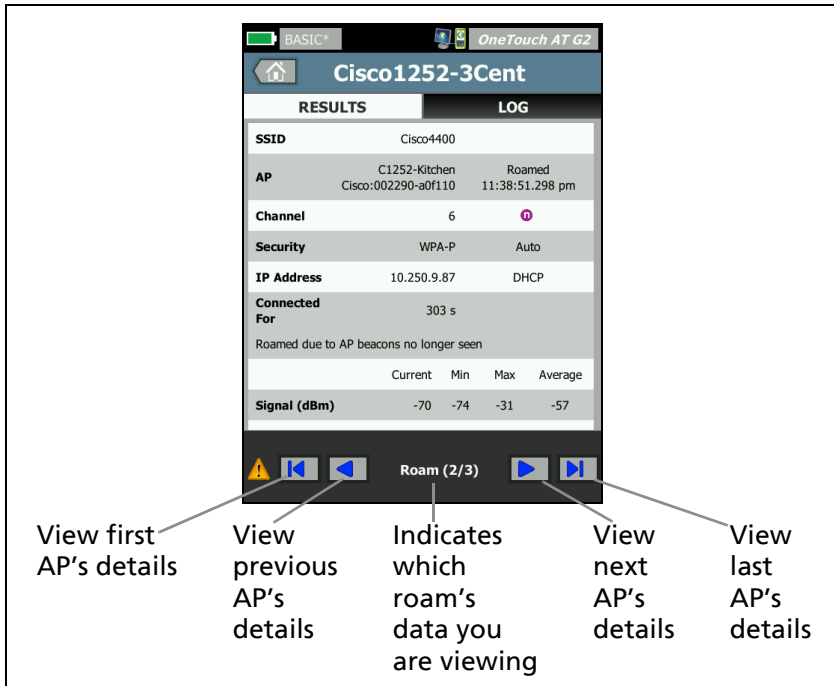


Figure 46. Roaming Navigation Controls

See also: "Connect Tool" on [page 238](#).

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 169](#).




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.

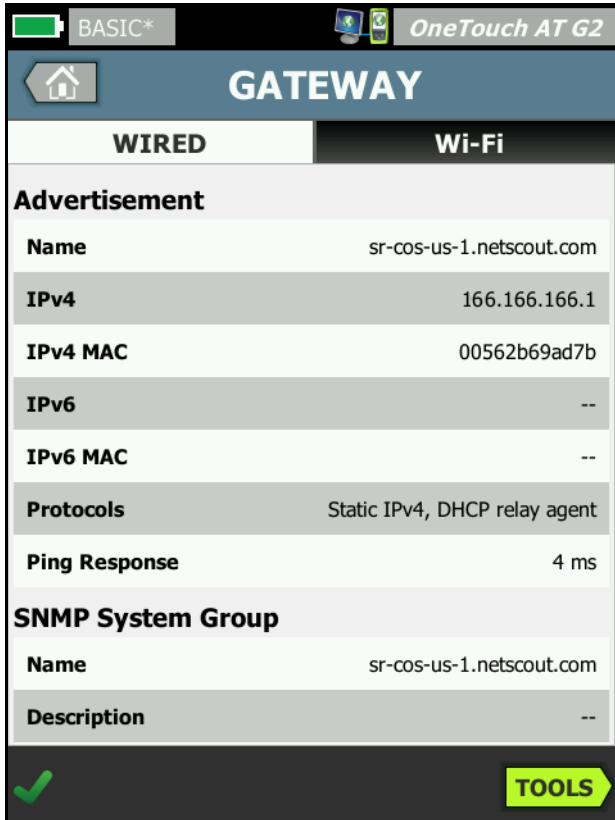


Figure 47. Gateway WIRED Tab

Wired gateway statistics are updated every 15 seconds.



Figure 48. 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 DHCP 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](#).

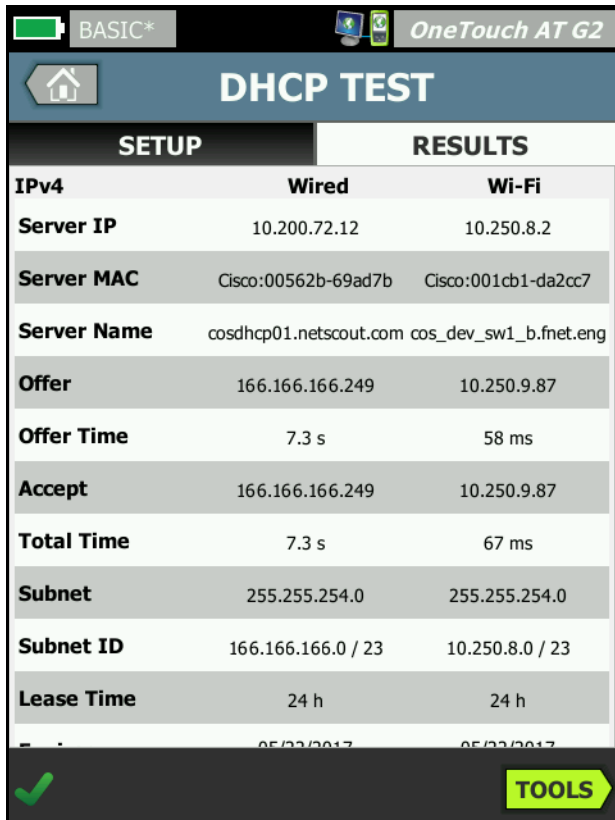
The **Time Limit** determines how much time can elapse before the OneTouch analyzer receives a response from the server. If the Time Limit is exceeded, the test will fail.

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



SETUP		RESULTS	
IPv4	Wired	Wi-Fi	
Server IP	10.200.72.12	10.250.8.2	
Server MAC	Cisco:00562b-69ad7b	Cisco:001cb1-da2cc7	
Server Name	cosdhcp01.netscout.com	cos_dev_sw1_b.fnet.eng	
Offer	166.166.166.249	10.250.9.87	
Offer Time	7.3 s	58 ms	
Accept	166.166.166.249	10.250.9.87	
Total Time	7.3 s	67 ms	
Subnet	255.255.254.0	255.255.254.0	
Subnet ID	166.166.166.0 / 23	10.250.8.0 / 23	
Lease Time	24 h	24 h	
	05/23/2017	05/23/2017	

Figure 49. 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.

Tools Button - Tap this button to run a path analysis to the DHCP server. When a second offer has been received, it is presented as a choice for path analysis, which can be used to help track down a rogue DHCP server.

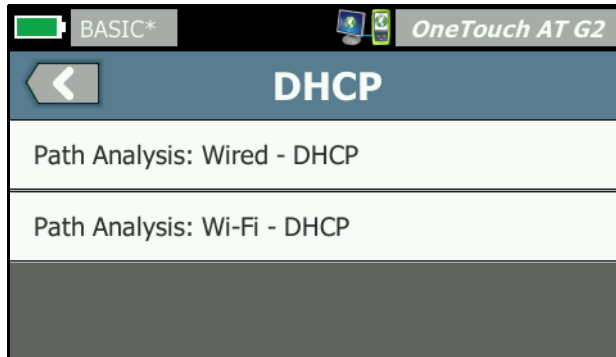


Figure 50. DHCP Path Analysis

DNS Server Test




Description

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

Configuration

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

- 1 On the HOME screen, tap the DNS server icon .
- 2 Tap the **SETUP** tab.
- 3 Tap the **Name** tab and enter the domain name to look up.

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

How it Works

The address of the DNS server is obtained through DHCP or by static configuration, via the wired connection, the 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.

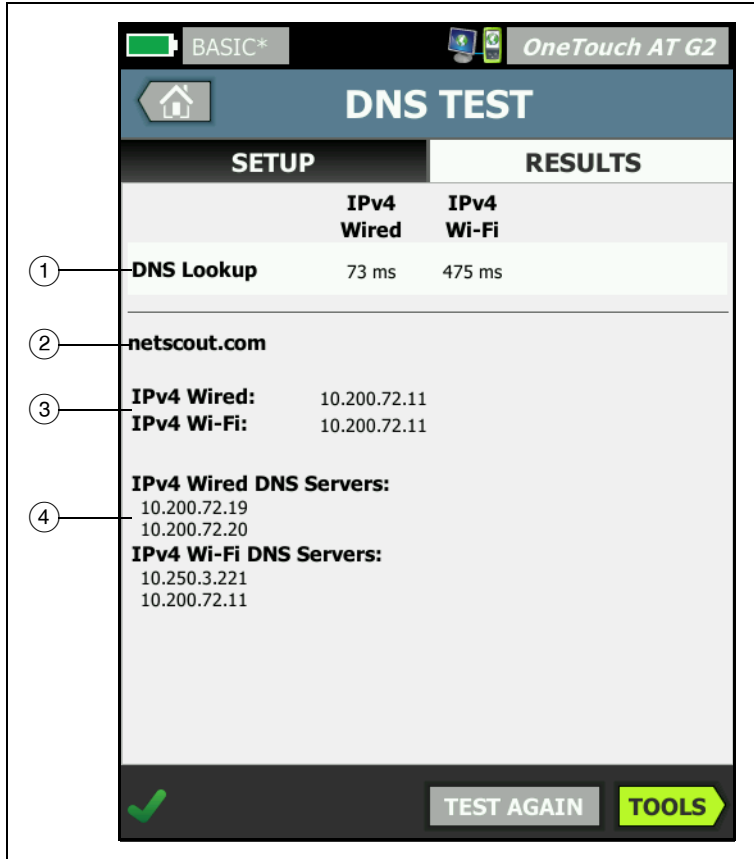


Figure 51. DNS Test Results

- 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 7: "Wired Analysis," beginning on [page 167](#) for details.

Chapter 5: User Tests

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

To Add a User Test

- 1 Tap and hold anywhere in a tier area on the HOME screen (see [page 19](#)). The list of User Tests is displayed.

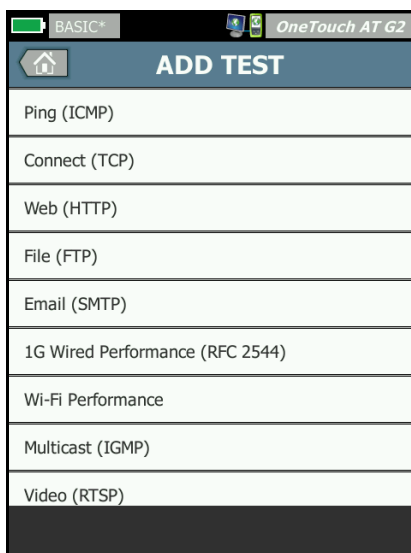


Figure 52. Add Test Screen

- 2 Select a test from the list and configure it on its SETUP tab.
- 3 Return to HOME. The new test is added to the HOME screen at the point where you tap and hold.

To Edit a User Test

- 1 Tap the test's icon on the HOME screen. Two tabs are displayed: SETUP and RESULTS.
- 2 Tap the SETUP tab and configure the test.

You can save user tests, along with other OneTouch analyzer settings, in a Profile. See "Profiles" on [page 161](#).

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 21](#).

For instructions on adding user tests, see "Adding User Tests" on [page 43](#).

See also: "Finding User Test Target Servers in Wired Analysis" on [page 176](#).

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

- [Ping \(ICMP\) Test, page 105](#)
- [Connect \(TCP\) Test, page 109](#)
- [Web \(HTTP\) Test, page 114](#)
- [File \(FTP\) Test, page 119](#)
- [Email \(SMTP\) Test, page 124](#)
- [Wired Performance Test, page 129](#)
- [Wi-Fi Performance Test, page 144](#)
- [Multicast \(IGMP\) Test, page 154](#)
- [Video \(RTSP\) Test, page 156](#)

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**.

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




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

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  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.

	RESULTS	
	IPv4 Wired	IPv4 Wi-Fi
DNS Lookup	21 ms	28 ms
Current	4 ms	6 ms
Sent	1	1
Received	1	1
Lost	0	0
Minimum	4 ms	6 ms
Maximum	4 ms	6 ms
Average	4 ms	6 ms
Return Code		
IPv4 Wired:	216.58.217.4	Class:00562b-60e7b

Figure 53. Ping Test Results

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

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

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

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

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

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




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



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

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

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

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

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

Tap the **TEST AGAIN** button  to re-run the test. Tap the **TOOLS** button  to run path analysis to the target server, launch a browser against the target server, or Telnet/SSH to the server.

Connect (TCP) Test



Purpose

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

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

Configuration

Server - Enter the URL or the IP address of the target server. See also: "Server" on [page 105](#).

Name - The Name button allows you to assign a custom name to the test. See also: "Name" on [page 105](#).



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.

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

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

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

In Continuous mode, the 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  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.

SETUP	RESULTS	
	IPv4 Wired	IPv4 Wi-Fi
DNS Lookup	23 ms	1 ms
Current	51 ms	52 ms
SYN Sent	1	1
ACK Received	1	1
ACK Lost	0	0
Minimum	51 ms	52 ms
Maximum	51 ms	52 ms
Average	51 ms	52 ms
Ping	--	--
Return Code		

Figure 54. 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  to re-run the test. Tap the **TOOLS** button  to run path analysis to the target server,

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

Web (HTTP) Test



Purpose

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

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

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

Configuration

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

By default, the HTTP test tries to reach the target server on port 80. To reach web servers that operate on a different port, type a colon (:) and specify the port number after the URL. For example, to reach a web server on port 8080 use the following format: `www.website_name.com:8080`. See also: "Server" on [page 105](#).



Name - The Name button allows you to assign a custom name to the test. See also: "Name" on [page 105](#).

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

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

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

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

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

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

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

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

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

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

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

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

How it Works

When you execute an HTTP test, the OneTouch AT analyzer:

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

Results

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

	IPv4 Wired	IPv4 Wi-Fi
DNS Lookup	<1 ms	20 ms
TCP Connect	53 ms	59 ms
Data Start	54 ms	57 ms
Data Transfer	161 ms	179 ms
Total Time	268 ms	315 ms
Data Bytes	62 K	62 K
Rate (bps)	3.1 M	2.8 M
Ping	--	--
Return Code	200	200
IPv4 Wired:	53.55.140.72	

Figure 55. Web (HTTP) Test Results

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

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

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

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

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

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

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

Rate is the data transfer rate.

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

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

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

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

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

Tap the **TEST AGAIN** button  to re-run the test. Tap the **TOOLS** button  to run path analysis to the target server, launch a browser against the target server, or Telnet/SSH to the server.

File (FTP) Test

Purpose

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

Configuration

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

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



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

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

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

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

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

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

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

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

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

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

If **Direction** is set to **Get**, File specifies the name of the file to be downloaded from the server. The file will be retrieved and the

size and data rate will be calculated. Data is discarded as soon as it is downloaded. It is not written to a file and it is not retained on the OneTouch analyzer.

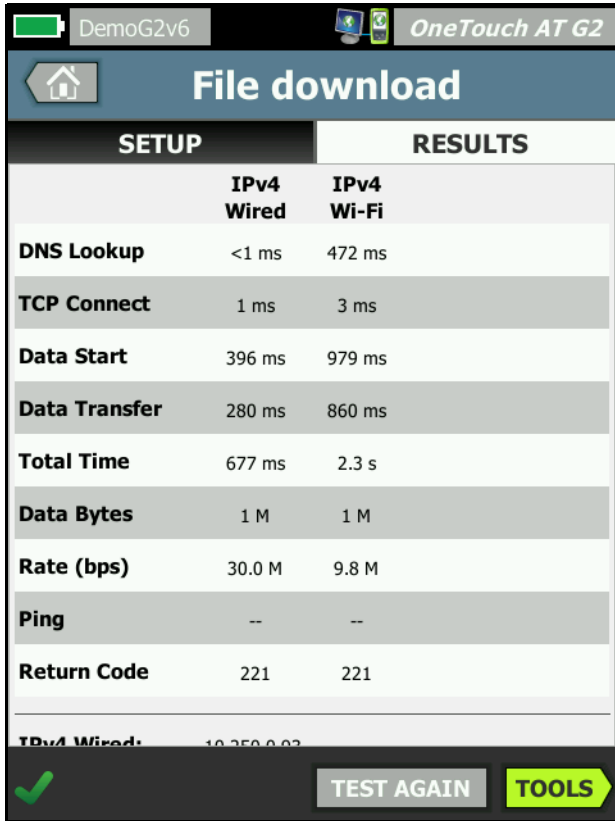
If **Direction** is set to **Put**, **File** specifies the name of the file that is created on the server. The size of the file is determined by the **Transfer Size** control. The file contains a text string that indicates the file was sent from the OneTouch analyzer. The text string is repeated to produce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



SETUP	RESULTS	
	IPv4 Wired	IPv4 Wi-Fi
DNS Lookup	<1 ms	472 ms
TCP Connect	1 ms	3 ms
Data Start	396 ms	979 ms
Data Transfer	280 ms	860 ms
Total Time	677 ms	2.3 s
Data Bytes	1 M	1 M
Rate (bps)	30.0 M	9.8 M
Ping	--	--
Return Code	221	221
IPv4 Wired:	10.250.0.03	

Figure 56. FTP Test Results

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

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

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

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

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

Data Bytes is the total number of data bytes transferred.




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

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

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

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

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

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

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

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

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 105](#).

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.

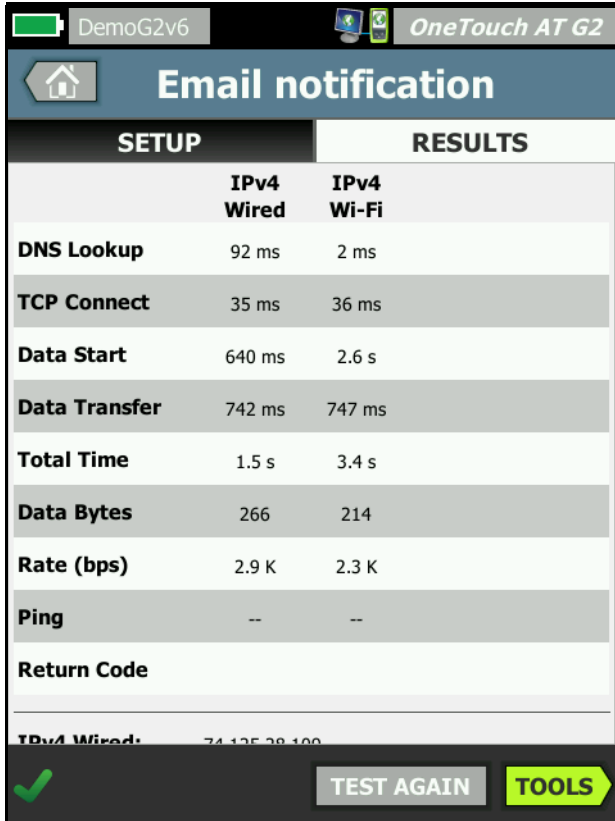
Login - If the SMTP server requires authentication, set **Login** to **On** and enter the username and password.

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.



SETUP	IPv4 Wired	IPv4 Wi-Fi
DNS Lookup	92 ms	2 ms
TCP Connect	35 ms	36 ms
Data Start	640 ms	2.6 s
Data Transfer	742 ms	747 ms
Total Time	1.5 s	3.4 s
Data Bytes	266	214
Rate (bps)	2.9 K	2.3 K
Ping	--	--
Return Code		
IPv4 Wired:	74.125.28.100	

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

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

```
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

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 roundtrip traffic.


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

To run this test:

- **Set up the peer or reflector for the test:**
 - See “To Configure a OneTouch AT analyzer as a Peer” on [page 131](#).
 - See “To Configure a LinkRunner AT (2000) as a Reflector” on [page 133](#).
 - See “To Configure a LinkRunner G2 as a Reflector” on [page 135](#).
 - See “To Use the NETSCOUT Network Performance Test (NPT) Reflector Software” on [page 135](#).
- **Set up the source OneTouch AT.** See “To Configure the Source OneTouch AT Analyzer” on [page 137](#).


To Configure a OneTouch AT analyzer as a Peer

Follow these steps to configure a peer (OneTouch AT, G2, or 10G 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.
- 4 Set the **Port** number, and turn **Enable AutoStart** on or off.

Port - Select the appropriate UDP port number. Whether you use the default port or select another port number, the port must not be blocked by network security. Note that you must select the same port in the source device.

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

- 5 Tap the **START** button . 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.

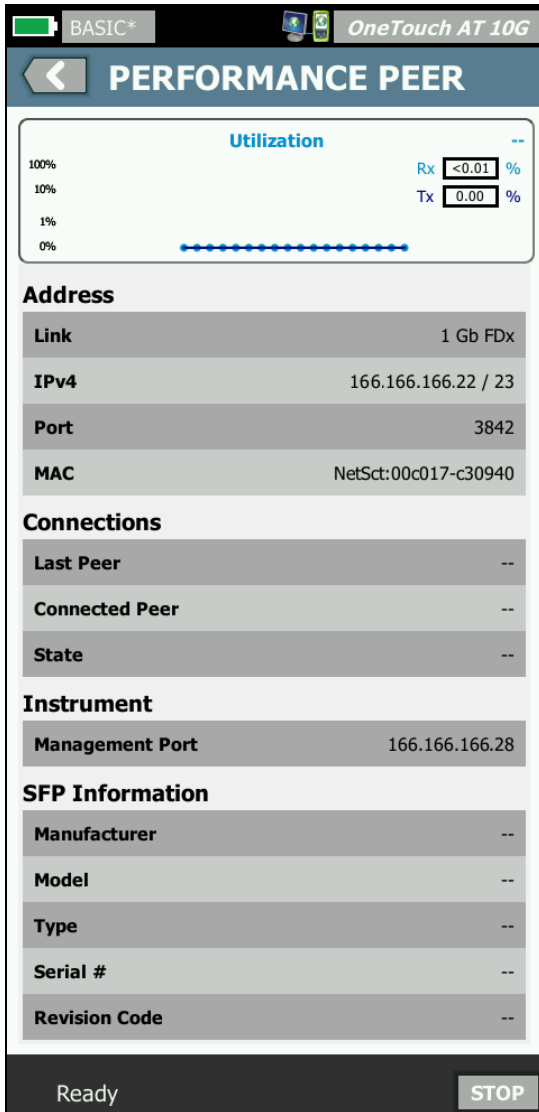


Figure 60. Wired Performance Test - Performance Peer Screen

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

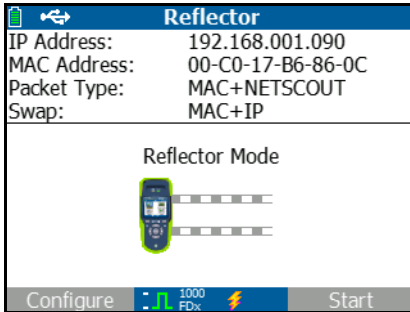
Note

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

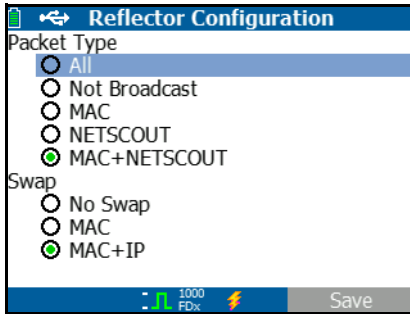
- 1 Connect the AC adapter to the LinkRunner AT (2000) or ensure that the battery has enough charge to complete the test.
- 2 On the LinkRunner AT 2000 home screen, select **Tools**.
- 3 Select **General Configuration**.
- 4 Under the Manage Power section, ensure that the **Auto Shutoff Enabled** check 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.



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



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

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

Caution

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

- 8 Select **Save**.

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

Refer to the LinkRunner AT User Manual for additional information.

To Configure a LinkRunner G2 as a Reflector

- 1 Connect the AC adapter to the LinkRunner G2 or ensure that the battery has enough charge to complete the test.
- 2 Start the LinkRunner G2 testing application.
- 3 To open the Reflector screen, touch the navigation menu icon at the top left of the LinkRunner G2 application screen, and then touch **Reflector**.
- 4 The LinkRunner will acquire an IP address. Note the IP address. You will enter this address when setting up the source analyzer.
- 5 Configure the **Packet Type** and **Swap** settings as required. The default settings **Packet Type: MAC + NETSCOUT** and **Swap: MAC + IP** are recommended.

Caution

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

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

Refer to the LinkRunner G2 User Guide for additional information.

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

Note

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

- 1 Download the free NETSCOUT NPT Reflector software onto a PC:
 - Download from <http://enterprise.netscout.com/support/downloads>
 - Or enter the OneTouch's Management Port IP address into a web browser to download the NPT Reflector Software from the OneTouch Web Server. See "Remote File Access Using a Web Browser" on [page 349](#).
- 2 Install the Reflector on your PC by running the .exe file.
- 3 Open the Reflector application.

Once the Reflector application is installed and opened on your PC, it automatically detects available network interfaces and their link status.
- 4 Check the box next to **Enable Reflection** for each network interface you want to use as a Reflector for your network performance test.
- 5 Leave the Reflector application window open on your PC during testing.

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

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 "Adding User Tests" on [page 43](#).

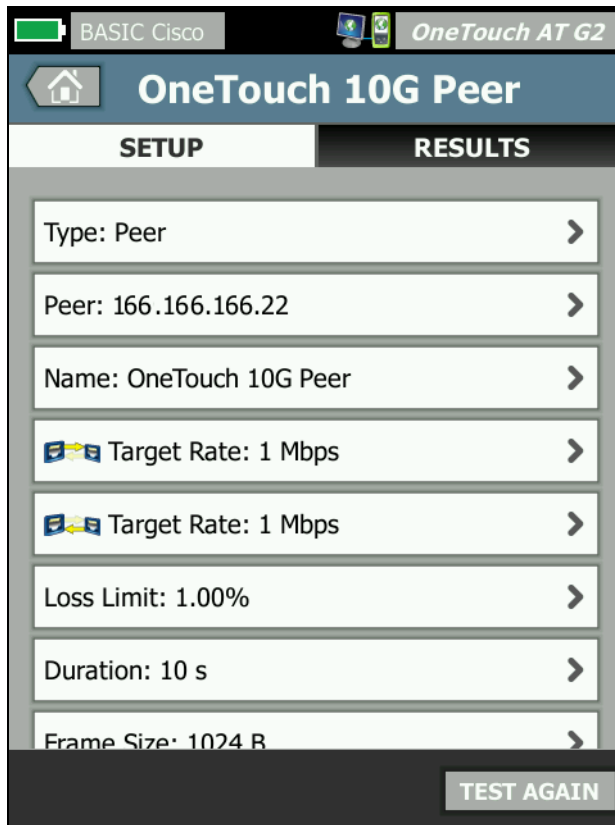




Figure 61. Wired Performance Test Setup Tab

- 3 Tap the **Type** button. Set the type to **Peer** or **Reflector**. See "Configuration" on [page 130](#).
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 105](#).
- 5  **Target 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.

 **Target 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 roundtrip traffic, and only one rate can be specified.

- 6 **Loss Limit:** 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 139](#).
- 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

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

For each test, a TCP control connection is established on the port specified in the test configuration. UDP packets are sent as test traffic. For the latency test, the next higher port (configured port +1) is used for exchanging latency measurement frames.

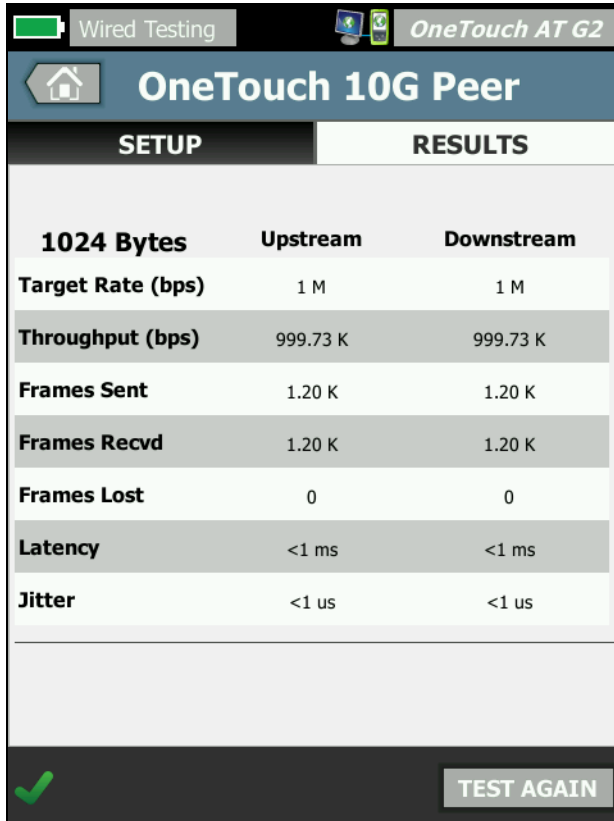
When using a peer endpoint (a OneTouch AT analyzer), separate upstream and downstream measurements are provided for rate, frames sent, frames received, and lost frames. Latency and jitter measurements are always made on the roundtrip.

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

Results

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

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



The screenshot shows the 'OneTouch 10G Peer' test results interface. At the top, it indicates 'Wired Testing' and 'OneTouch AT G2'. The main title is 'OneTouch 10G Peer'. Below the title, there are two tabs: 'SETUP' and 'RESULTS'. The 'RESULTS' tab is active, displaying a table of performance metrics for a 1024 Bytes frame size. The table has three columns: '1024 Bytes', 'Upstream', and 'Downstream'. The metrics include Target Rate (bps), Throughput (bps), Frames Sent, Frames Recvd, Frames Lost, Latency, and Jitter. A green checkmark is visible in the bottom left corner, and a 'TEST AGAIN' button is in the bottom right corner.

1024 Bytes	Upstream	Downstream
Target Rate (bps)	1 M	1 M
Throughput (bps)	999.73 K	999.73 K
Frames Sent	1.20 K	1.20 K
Frames Recvd	1.20 K	1.20 K
Frames Lost	0	0
Latency	<1 ms	<1 ms
Jitter	<1 us	<1 us

Figure 62. 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.

OneTouch 10G Peer		
SETUP	RESULTS	
64 Bytes	Upstream	Downstream
Target Rate (bps)	1 M	1 M
Throughput (bps)	999.60 K	998.66 K
Frames Sent	14.88 K	14.88 K
Frames Recvd	14.88 K	14.88 K
Frames Lost	0	0
Latency	<1 ms	<1 ms
Jitter	23.94 us	23.94 us
128 Bytes	Upstream	Downstream
Target Rate (bps)	1 M	1 M
Throughput (bps)	999.41 K	998.93 K

Figure 63. 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.

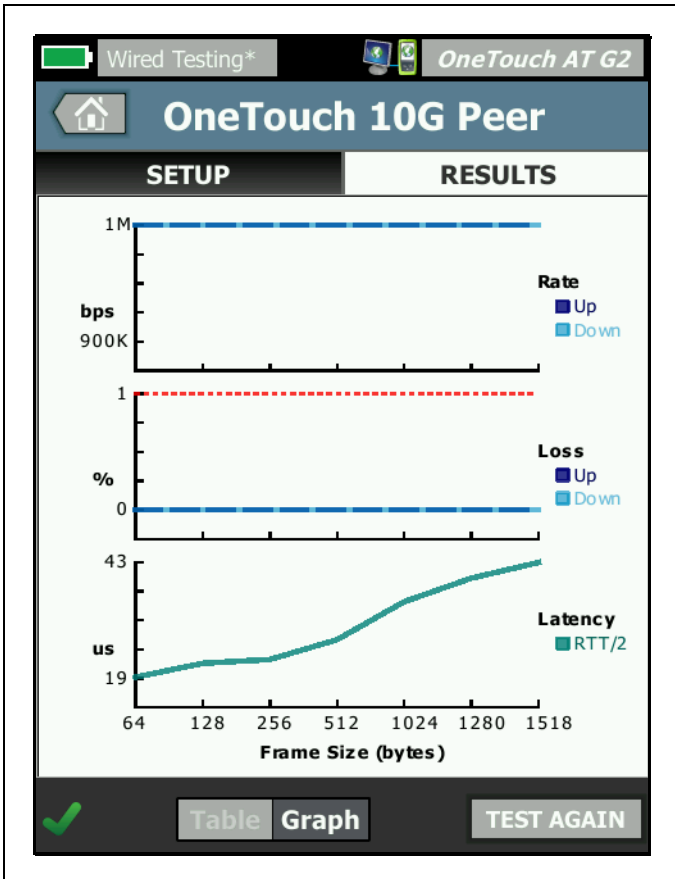


Figure 64. Test Results: RFC 2544 Sweep, Graphical View

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

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

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

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

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

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 roundtrip time is measured, then divided by two to provide upstream and downstream values.

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

Jitter Measurement



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

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

Reflector Jitter Measurement - When using a reflector endpoint, jitter is the arithmetic range (the difference between the largest value and the smallest value) of variation in twenty successive latency measurements.

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

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

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

✘ A red x indicates the test failed.

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

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 it 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.

Rates are user configurable up to 600 Mbps in both directions (upstream/downstream) for Peer and "This OneTouch" test types and roundtrip for the Reflector test type. Achievable rates will vary depending on the Wi-Fi environment but may be up to 600 Mbps for the Peer and Reflector test types and up to 100 Mbps for "This OneTouch" 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 roundtrip traffic.

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

To run this test:

- **Set up the peer or reflector for the test:**
 - See “To Configure a OneTouch AT analyzer as a Peer” on [page 131](#).
 - See “To Configure a LinkRunner AT (2000) as a Reflector” on [page 133](#).
 - See “To Configure a LinkRunner G2 as a Reflector” on [page 135](#).
 - See “To Use the NETSCOUT Network Performance Test (NPT) Reflector Software” on [page 135](#).
- **Set up the source OneTouch AT.** See “Configure the Source OneTouch AT Analyzer” on [page 146](#).

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.




Figure 65. Wi-Fi Performance 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 130](#).

The **Name** button allows you to assign a custom name to the test. See also: "Name" on [page 105](#).

 **Target Rate** - This is the requested rate of upstream traffic. Valid rates are from 1 Mbps to 600 Mbps.

 **Target Rate** - This is the requested rate of downstream traffic. Valid rates are from 1 Mbps to 600 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 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 base port used by the test.


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 130](#).

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 105](#).

 **Target Rate** - This is the rate of traffic from the Wi-Fi connection to the wired connection. Valid rates are from 1 Mbps to 600 Mbps.

 **Target Rate** - This is the rate of traffic from the wired connection to the Wi-Fi connection. Valid rates are from 1 Mbps to 600 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 base port used by the test.


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 130](#).

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 105](#).

 **Target Rate** - When using a reflector, upstream and downstream traffic are not individually measured. Results are based on roundtrip traffic, and only one rate can be specified. Maximum configurable rate is 600 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 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 base port used by the test.

Run the Test

To run the test, ensure that you have started the endpoint, then start the Wi-Fi Performance Test by tapping AutoTest or TEST AGAIN on the Wi-Fi Performance Test RESULTS tab.

How it Works

A TCP control connection is only established during a Peer test on the specified port for traffic from the Wi-Fi interface to the wired interface. Only the Peer test type establishes 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.

For 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.

For 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.

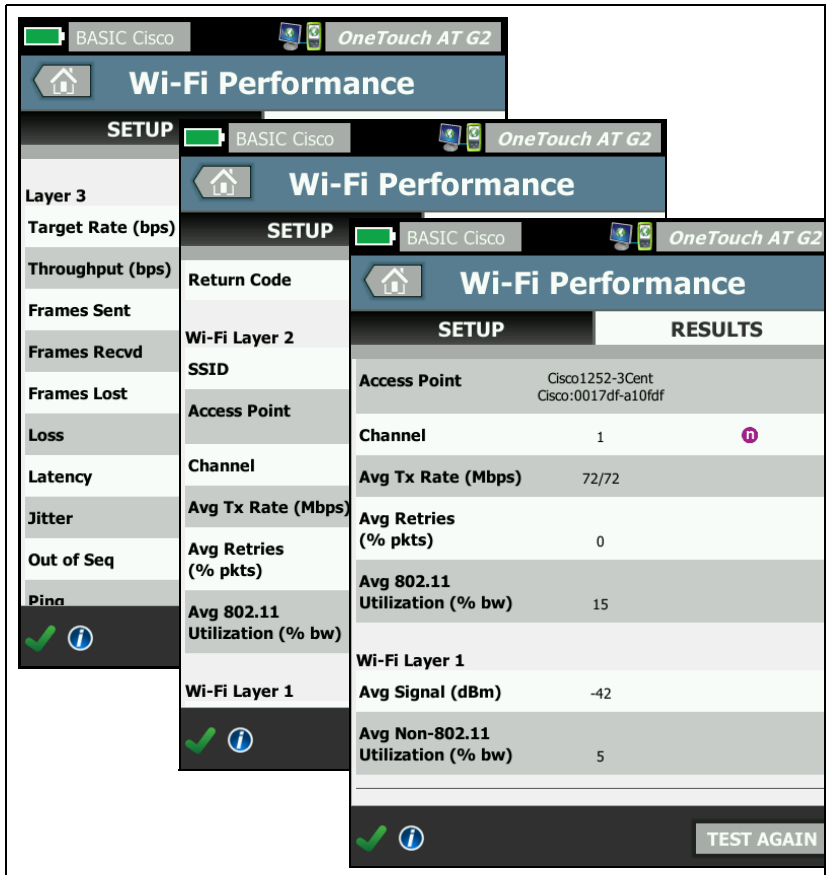


Figure 66. Wi-Fi Performance Test Results

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.

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

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

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.

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.

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

Channel - The channel number is shown. If a bonded channel is used, the word “Bonded” appears here.

Avg Tx Rate (Mbps) - 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.

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

Avg 802.11 Utilization (% bw) - 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 250](#).

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

Avg Non-802.11 Utilization (% bw) - 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  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 105](#).

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 154](#).

		10.1.110.11	
	SETUP	RESULTS	
		IPv4 Wired	IPv4 Wi-Fi
Data Start		165 ms	563 ms
Data Transfer		165 ms	190 ms
Total Time		329 ms	756 ms
Data Bytes		21 K	20 K
Rate (bps)		1.0 M	863.2 K
Return Code		700	700
IPv4 Wired:		10.250.0.93	
IPv4 Wi-Fi:		10.250.0.93	

TEST AGAIN

Figure 67. 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  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 105](#).

The **Name** button allows you to assign a custom name to the test. See also: "Name" on [page 105](#).

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.

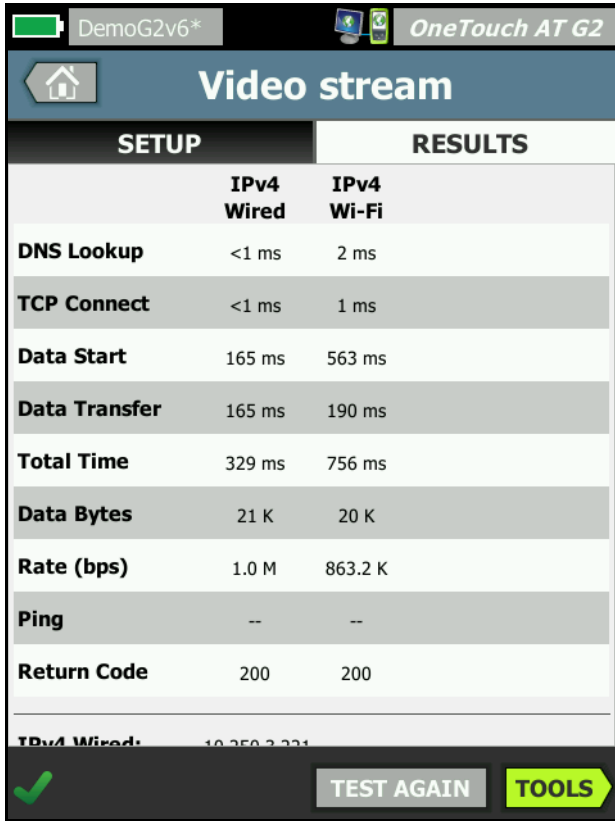
File is the name of the file that will be received (streamed).

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.



	RESULTS	
	IPv4 Wired	IPv4 Wi-Fi
DNS Lookup	<1 ms	2 ms
TCP Connect	<1 ms	1 ms
Data Start	165 ms	563 ms
Data Transfer	165 ms	190 ms
Total Time	329 ms	756 ms
Data Bytes	21 K	20 K
Rate (bps)	1.0 M	863.2 K
Ping	--	--
Return Code	200	200
IPv4 Wired:	10.250.2.221	

Figure 68. 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  to re-run the test. Tap the **TOOLS** button  to run path analysis to the target server, launch a browser against the target server, or Telnet/SSH to the server.

Chapter 6: 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

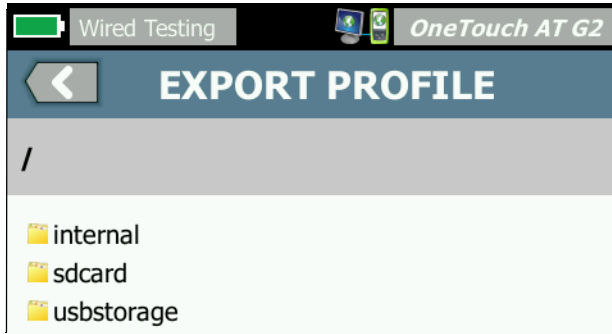
To import or export a group of Profiles quickly, use FTP or the Cloud Service, or map the analyzer's user file system as a network drive.

- See "Remote File Access Using an FTP Client" on [page 351](#).
- See "Remote Access from the Cloud" on [page 365](#).
- See "Remote File Access Using a Mapped Network Drive (WebDAV)" on [page 351](#).

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 341](#).) 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 7: 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.



Figure 69. 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 25](#).
- 3 Tap the **SNMP v3** button and add v3 credentials.

Slow Discovery

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

How Wired Analysis Works

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

Devices are discovered using active and passive analysis methods.

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

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

Results

The number of discovered devices is shown under the Wired



Analysis icon on the HOME screen. Tap the icon to display the WIRED ANALYSIS summary screen.

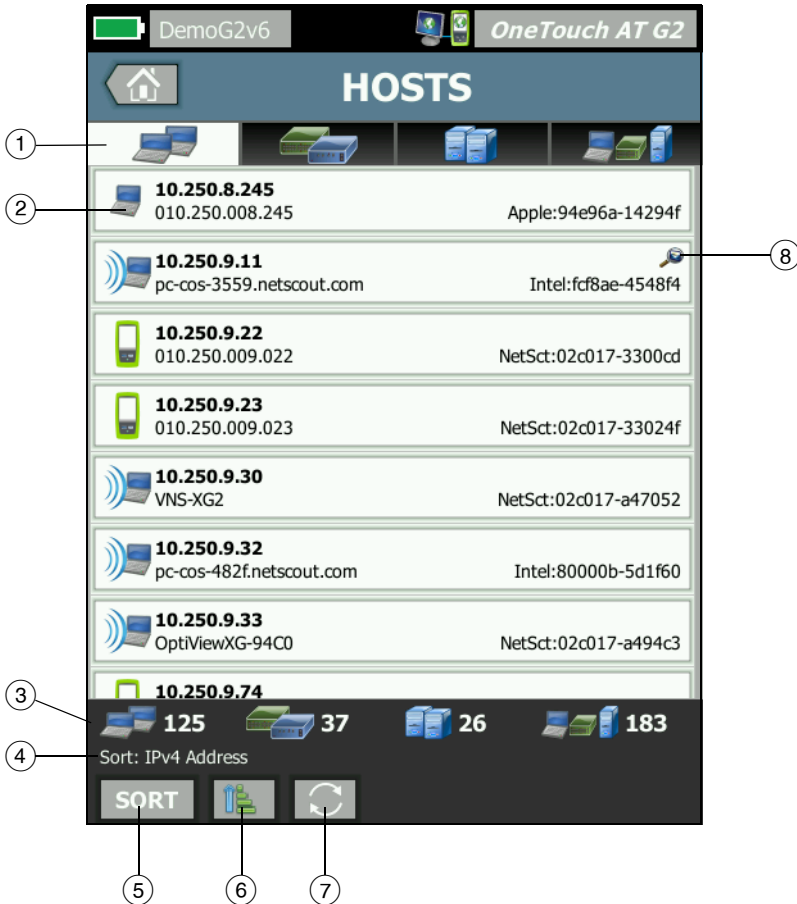


Figure 70. WIRED ANALYSIS Screen

- ① The HOSTS, ACCESS DEVICES, and SERVERS tabs let you filter the Wired Analysis results. Access devices are switches, routers, etc. The ALL DEVICES tab displays devices in all three categories.
- ② Each device is displayed on a button. An icon at the left side of the button indicates the device type.



Wired host



Switch



Router



Server



Printer



NETSCOUT tool



VoIP call manager or VoIP TFTP server



VoIP phone



Virtual switch



Virtual machine



Hypervisor



Wireless LAN controller



Wireless access point



Wi-Fi client

The information displayed on device buttons changes based

on the sort key.

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








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



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

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

- ③ The status bar is displayed on all WIRED ANALYSIS screens. It shows the number of hosts, access devices, and servers found. It also shows the total number of devices discovered.
- ④ The currently selected sort key is displayed above the **SORT** button .
- ⑤ The **SORT** button  lets you sort the list of hosts, access devices, servers, or all devices. See “Wired Device Sorts” on [page 175](#).
- 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.
- ⑧ The presence of a Cross-link Discovery icon indicates that the device was discovered during both Wi-Fi and Wired Analysis. It also indicates the ability to view the Wi-Fi Analysis data from Wired Analysis, and the Wired Analysis data from Wi-Fi Analysis.

To Show Wired Device Details

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

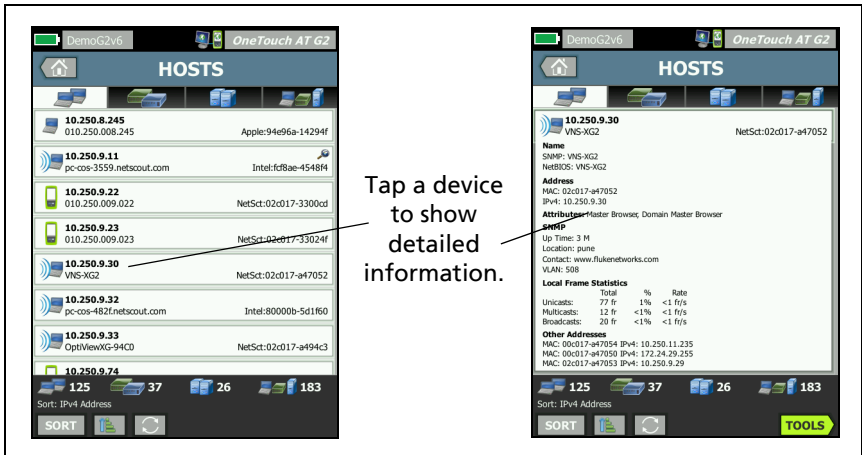


Figure 71. Displaying Wired Device Details

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

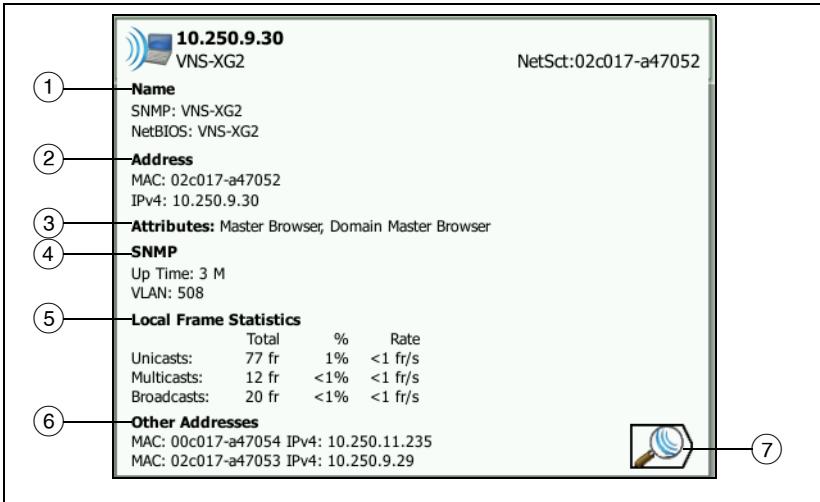




Figure 72. Wired Device Details

- ① This shows the device's best name in bold characters. It shows additional address information if available.
- ② The device's IP addresses
- ③ The server's attributes (e.g. virtual machine, hypervisor, domain controller, HTTP, SMTP, MS Exchange, Oracle, etc.)
- ④ Information gathered via SNMP is displayed here if available.
- ⑤ Local Frame Statistics provides the following information for unicasts, multicasts, and broadcasts:

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

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

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

- ⑥ Shows all the other IP addresses that are associated with the device, if any. Scroll down the screen to view any additional addresses, if available.
- ⑦ 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 button 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
- Cross-link Discovery - displays devices that were discovered during both Wi-Fi and Wired Analysis.
- 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 AP
- Lightweight wireless
- Wireless LAN controller
- Wi-Fi client
- Wireless access point
- Netscout tool
- Printer
- Switch
- Router
- Client
- Domain - An alphabetic sort based on the Windows NetBIOS domain name
- Top Unicast - A numerical sort based on the number of unicast frames sent
- Top Multicast - A numerical sort based on the number of multicast frames sent
- Top Broadcast - A numerical sort based on the number of broadcast frames sent
- Switch Name/Slot/Port - An alphabetic sort based on the switch's best name, slot, and port
- VLAN - A numerical sort based on VLAN number

Finding User Test Target Servers 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 .
- 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  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 .

- 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)

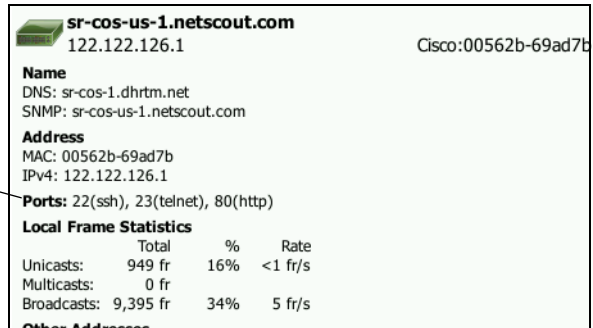


Figure 73. Port Scan Results

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) trace route measurement with a view of the path through the Layer 2 switches. SNMP queries are used to discover all switches. When the measurement is complete, the number of hops to the last device is shown. A maximum of 30 hops can be reported.

Running Path Analysis from the Wired Device Discovery Screen

- 1 To obtain details of SNMP-enabled devices, configure SNMP community strings or credentials for the network under test. See “SNMP” on [page 169](#).
- 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  appears at the lower-right corner of the screen.

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

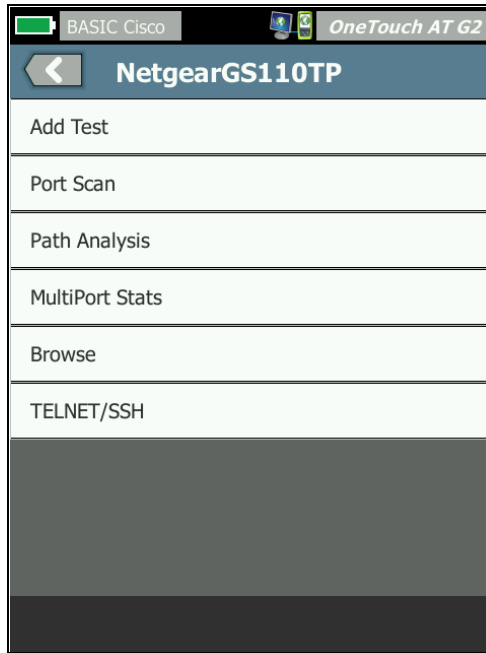


Figure 74. Wired Analysis Tools Menu

- 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 175](#).
- Each queried device's response time is shown at the right side of the button.

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

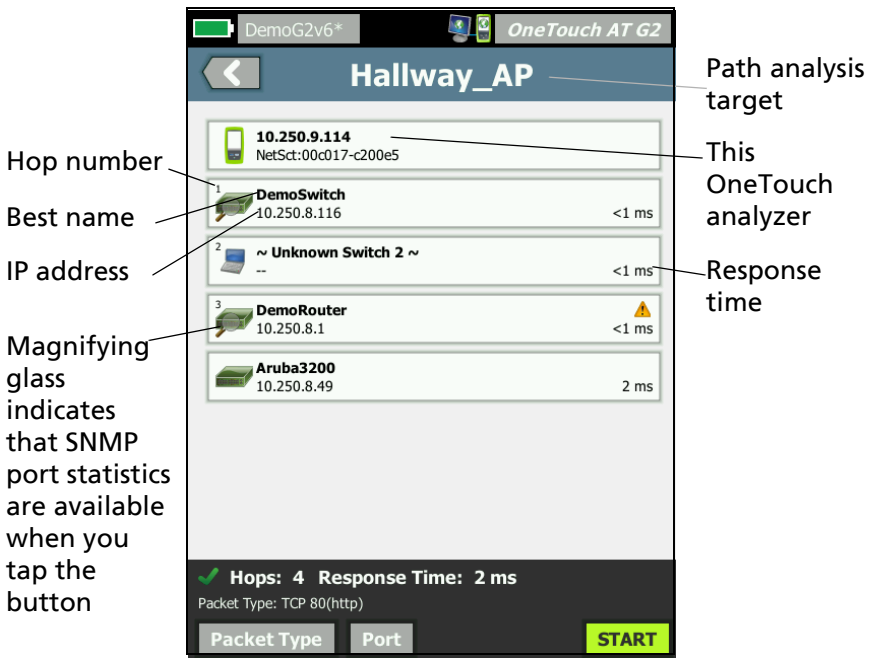





Figure 75. Path Analysis Results

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

- A progress spinner , indicating the test is in progress, a green check mark , indicating the test passed, or a red X , indicating the test failed
- The number of hops it took to reach the destination
- The response time of the last hop displayed in the list
- The packet type used for path analysis
- The Packet Type button, which appears when path analysis completes or is stopped

Tap the button to change the protocol used for path analysis. Available protocols are UDP, TCP, and ICMP. The default protocol is UDP. When using TCP, the default port is 80.

The TCP protocol uses TCP SYN packets for path analysis, which often produces the best results.

- 8 Tap a device's button to see detailed information. Details such as utilization and errors are shown for SNMP-enabled devices.

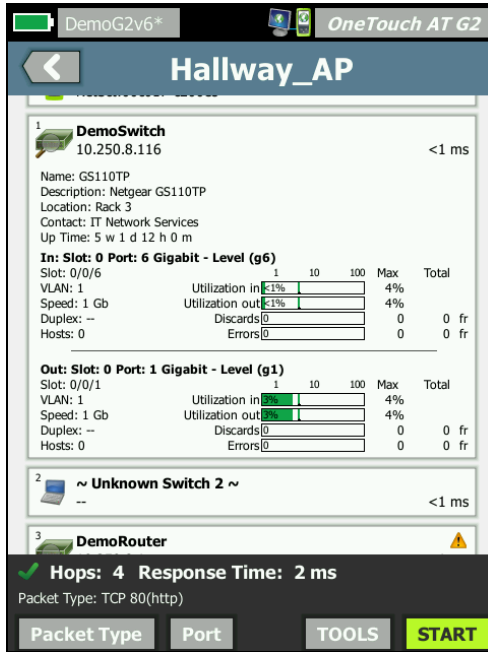


Figure 76. Path Analysis - Detailed Results

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 169](#).



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 167](#).



- 1 Tap the Wired Analysis icon  on the HOME screen.
- 2 On the WIRED ANALYSIS screen, tap a device's button to expand it.
- 3 Tap the TOOLS  button.




If the 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 77. MultiPort Statistics Button on Wired Analysis Tools Menu

- 4 Tap the **MultiPort Stats** button to display the device's port statistics.

MultiPort Statistics via the HOME Screen

- 1 On the HOME screen, tap the nearest switch icon  or the gateway icon .
- 2 Tap the TOOLS button  to display the tools available to the device. If the **MultiPort Stats** button is shown, it means that SNMP is configured on the device and you will be able to view its multiport statistics.
- 3 Select the **MultiPort Stats** button.

MultiPort Statistics via Path Analysis

Path analysis is described beginning on [page 179](#).


- 1 From the path analysis results screen, tap a device's button to expand it and view its details.
- 2 Tap the TOOLS button , which is at the bottom of the screen. If MultiPort Statistics are available for the device the **MultiPort Stats** button is displayed.



Figure 78. MultiPort Statistics Button on Path Analysis Tools Menu

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

If the **MultiPort Stats** button is shown, it means that SNMP is configured on the device and you will be able to view its mul-

tiport 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.

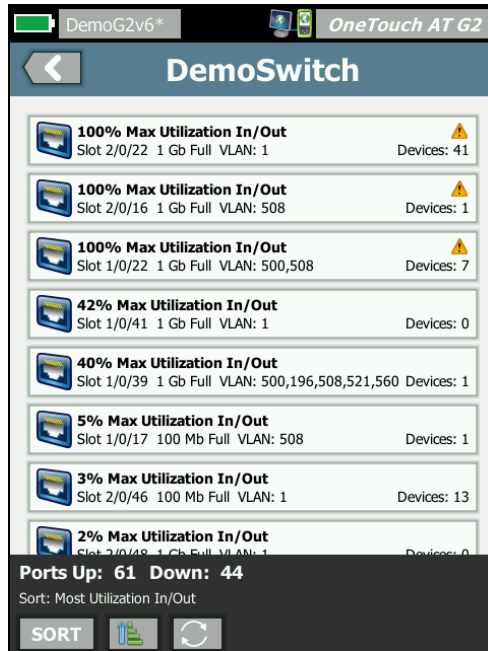


Figure 79. MultiPort Statistics Summary Screen

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

OneTouch AT and OneTouch AT G2 User Manual

- Slot number, port number
- Speed
- Duplex mode
- Problems (problem severity)
- Utilization In/Out
- Utilization In
- Utilization Out
- VLAN number
- Device Count (number of connected devices)

Use the Sort Order button to sort the results in ascending  or descending  order.

The **REFRESH** button  clears the results and restarts MultiPort analysis.

MultiPort Statistics Port Details Screen

Tap a port's button to expand it and view its details.

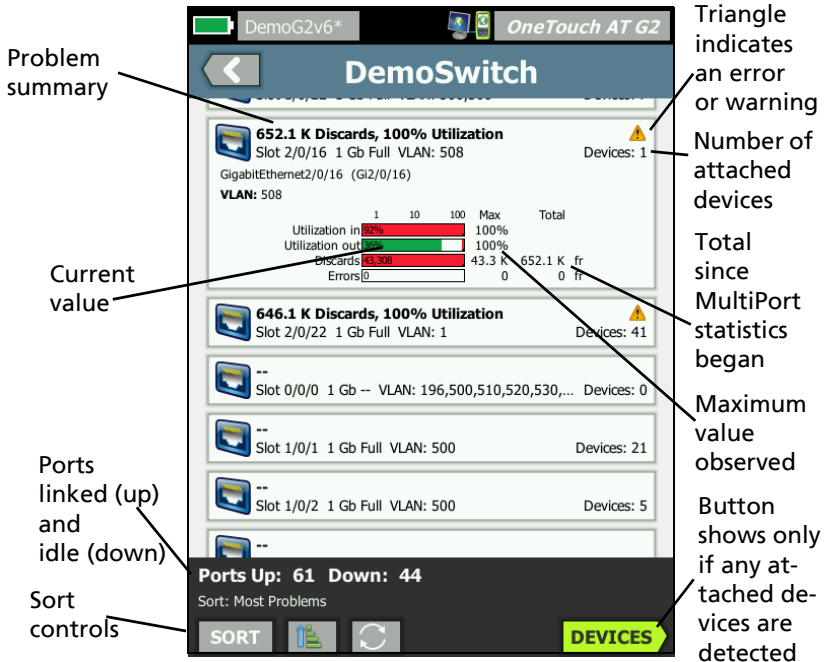


Figure 80. MultiPort Statistics Details Screen

Warning Triangle ⚠ - The warning triangle appears when (in or out) utilization is 70% or more, or when discards or errors occur.

Thresholds - The utilization bars and lines turn yellow at 40%; red at 70%. Discard error bars and lines are always shown in red.

Devices button - This button will only be shown if any attached devices are detected on the selected port. Selecting this button will show a listing of all the attached devices.

MultiPort Statistics Devices on Port Details Screen

Selecting the **Devices** button will show a listing of all attached devices on the current port. If you select a device that is SNMP

enabled, a **TOOLS** button will be shown at the bottom right of the screen.



Figure 81. MultiPort - Device on Port Details Screen

Choosing the **TOOLS** button will present you with a listing of available tools.

Web Browser

When you tap the **Browse** button, the browser is launched with the selected device as the target server. See "Browser" on [page 292](#).

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 294](#).

Chapter 8: 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/ac technologies, operating in both the 2.4 GHz and 5 GHz bands.

OneTouch AT G2 Additional Wi-Fi Features

The following Wi-Fi capabilities are supported only by the OneTouch AT G2:

- 802.11ac analysis and connection - OneTouch AT G2 includes 802.11ac data on Wi-Fi analysis screens and is able to Connect to 802.11ac access points.
- Identification of non-802.11 utilization - OneTouch AT G2 distinguishes between 802.11 utilization and non-802.11 utilization. See "AP Details" on [page 207](#).
- Wi-Fi Interferer detection and analysis - OneTouch AT G2 displays observed interfering devices on the Interferers tab. See "Interferer Analysis" on [page 228](#).

Wi-Fi must be enabled for Wi-Fi analysis to begin.

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 48](#).

Enable Connect Mode

When **Enable Connect** is **On** the analyzer attempts to connect to the configured network when AutoTest runs. See “Wi-Fi Network Connect Test” on [page 86](#).

When **Enable Connect** is **Off** 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 **Enable Connect** to **On** or **Off**.

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



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

Access Point Icon

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



See “Wi-Fi Network Connect Test” on [page 86](#).

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 channel 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.

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 6: "Profiles," beginning on [page 161](#).

- 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 Analysis Screens

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

- NETWORKS

- ACCESS POINTS
- CLIENTS
- CHANNELS
- INTERFERERS

Tap a tab to display the corresponding analysis screen.

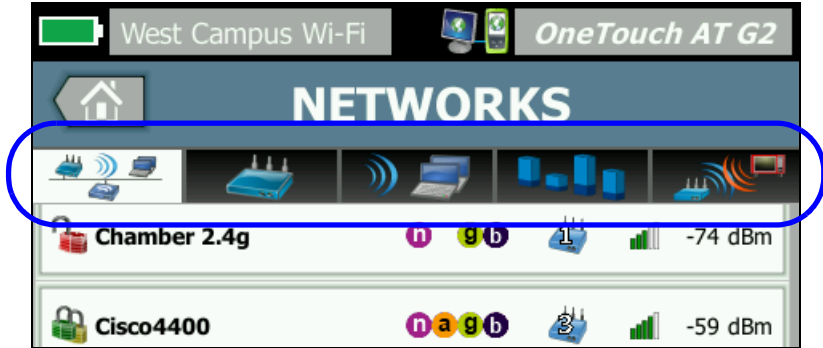


Figure 82. Wi-Fi Analysis Tabs

Network Analysis

The NETWORK analysis tab provides:

- A sortable list of all discovered Wi-Fi networks with summary information for each network (See Figure 83)
- A graphical representation of network coverage and important network details
- Filter buttons that provide deeper analysis of each network's access points, clients, channels, and interferers

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

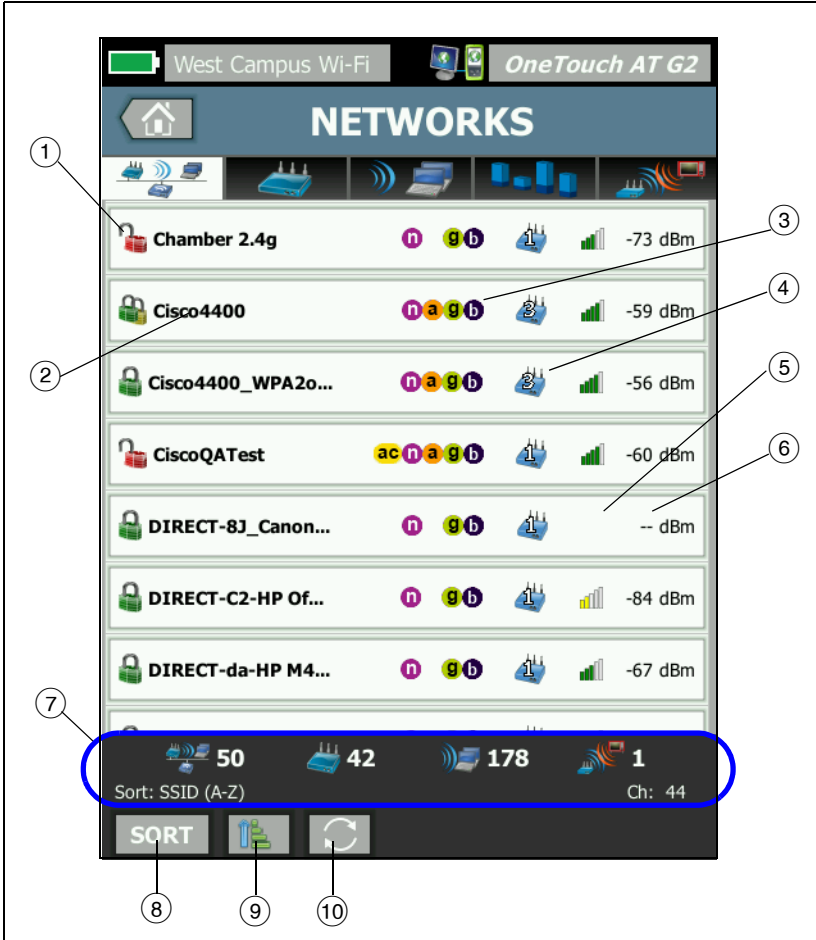
















Figure 83. Wi-Fi Network Analysis Tab, Sorted by SSID

- 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 202](#).
- 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 These icons indicate the 802.11 type(s) of APs configured for the networks detected by OneTouch. The 802.11 types in ascending order are 802.11b, 802.11g, 802.11a, 802.11n, and 802.11ac.
- ④ This icon changes based on the sort key that you select after tapping the SORT button . The access point icon  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.
- ⑤ 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

- ⑥ 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.
- ⑦ The status bar is displayed on all Wi-Fi ANALYSIS screens. It shows the number of networks (SSIDs), access points, clients, and interferers found.




This area also shows the current selected **Sort**: key on the left and channel numbers as they are scanned on the right.

- 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)
 - 802.11 Type

If the sort key is text, it is bold.



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.

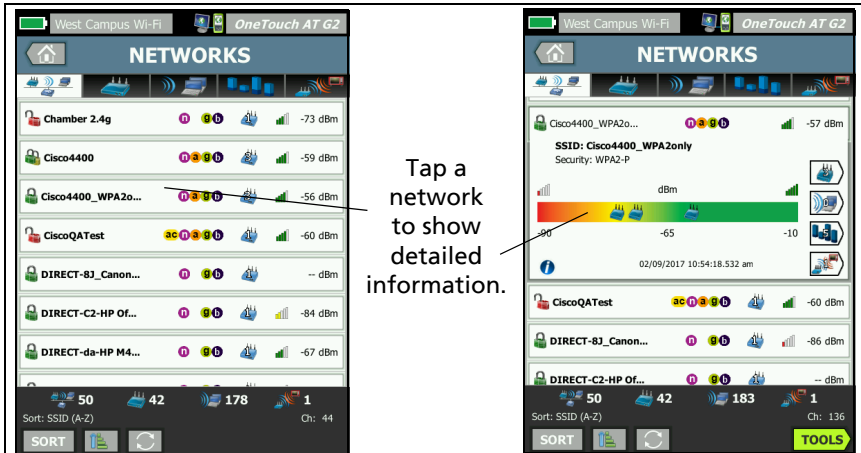


Figure 84. Displaying Wi-Fi Network Details

Network Details

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

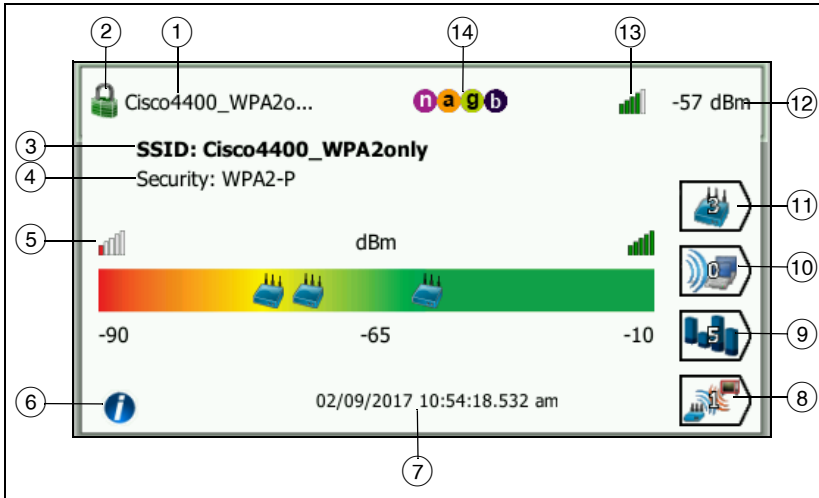


Figure 85. Wi-Fi Network Details

- 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 199](#) 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 -90 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 Interferer Filter Button to show a summary of non-802.11 devices detected on the network. Tap the **SHOW ALL** button to show all interferers again.
- ⑨ Tap the Channel Filter Button to show a summary of the channels the network is using. Tap the **SHOW ALL** button to show all channels again.
- ⑩ Tap the Client Filter Button to show a summary of the clients discovered on the network. Tap the **SHOW ALL** button to show all clients again.
- ⑪ Tap the AP Filter Button to show a summary of the APs configured for the network. Tap the **SHOW ALL** button to show all APs again.
- ⑫ 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.
- ⑬ The signal strength icon provides a quick visual indication of the network's signal strength as measured by the OneTouch analyzer. See [page 199](#) for a list of the thresholds that change the icon's appearance.
- ⑭ These icons indicate the 802.11 type(s) of APs configured for the networks detected by OneTouch. The 802.11 types in ascending order are 802.11b, 802.11g, 802.11a, 802.11n, and 802.11ac.

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

Access Point Analysis

The Access Point (AP) analysis tab provides:

- A sortable list of all discovered APs with summary information for each AP (See Figure 86).
- A graphical representation of AP details and trended measurements
- Filter buttons that provide deeper analysis of each AP's supported networks, associated clients, channels used, and detected interferers

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

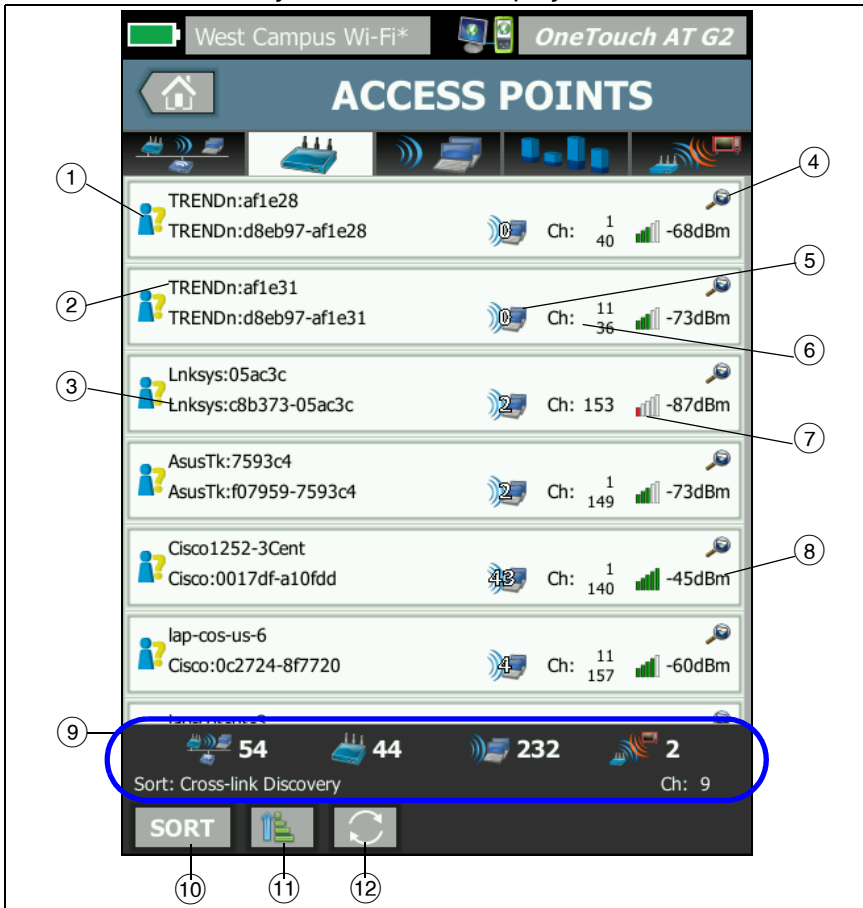



Figure 86. AP Analysis Tab




- 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 The presence of a Cross-link Discovery icon indicates device discovery during both Wi-Fi and Wired Analysis.
- ⑤ This shows the number of clients associated to the AP.
- ⑥ This changes based on the sort key that you select after tapping the SORT button . 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, and 802.11ac.
- ⑦ The signal strength icon provides a quick visual indication of the AP's signal strength as measured by the OneTouch analyzer. See [page 199](#) for a list of the thresholds that change the icon's appearance.
- ⑧ 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. If the AP has not been detected recently, the value is shown in gray text instead of black.

- ⑨ The status bar is displayed on all Wi-Fi ANALYSIS screens. It shows the number of networks (SSIDs), access points, clients, and interferers found.

This area also shows the current selected **Sort**: key on the left and channel numbers as they are scanned on the right.

- 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)
 - Cross-link Discovery (displays devices that were discovered during both, Wi-Fi and Wired Analysis).
 - 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.

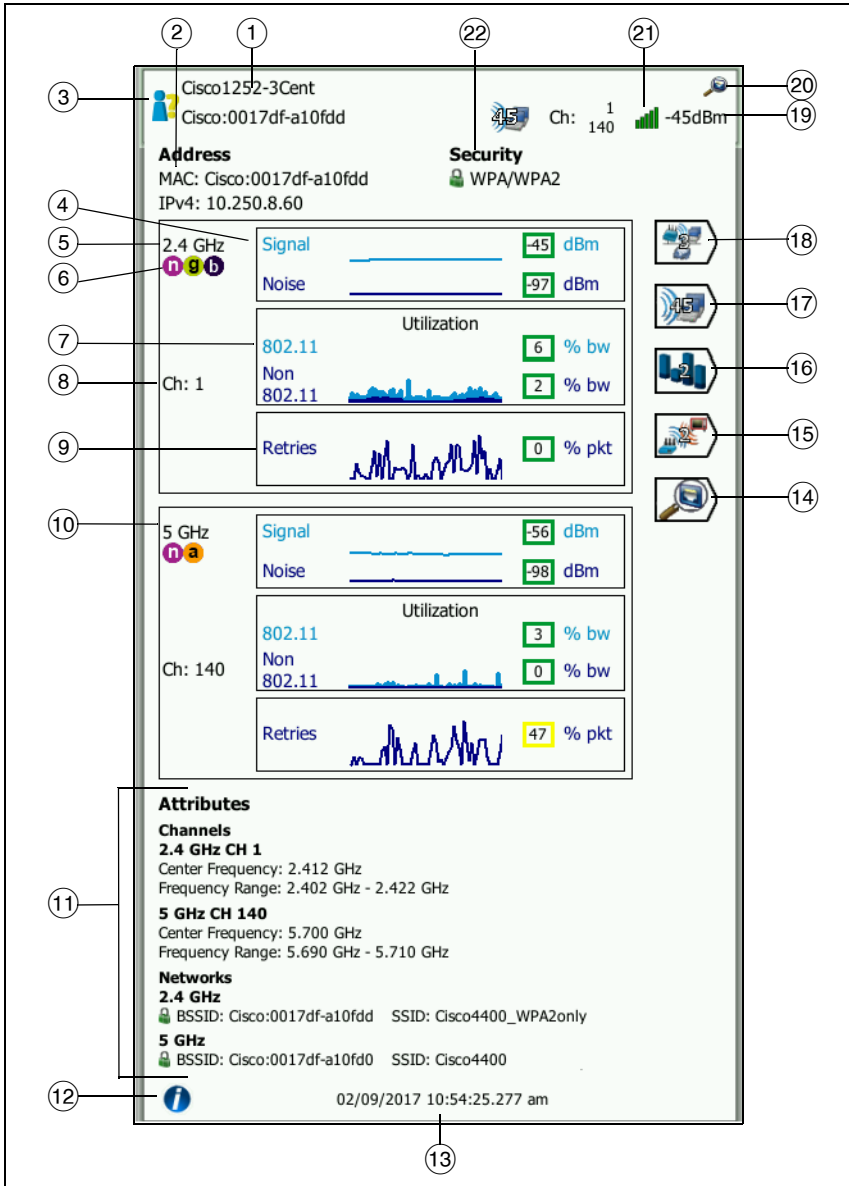


Figure 87. AP Details

- 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 addresses are shown here. For APs that support Cisco extensions, an IP address is available. 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.
- ③ This icon indicates the AP's Authorization Status. See [page 205](#).
Note that the *network's* security type (e.g. WPA-Enterprise) is shown in the network detail screen. See [page 202](#).
- ④ 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.
- ⑤ The band that the AP is using is displayed.
- ⑥ The supported 802.11 types of the AP are shown here.
- ⑦ The 802.11 utilization graph represents the AP's traffic on the respective channel.

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.
- ⑧ The channel(s) that the AP is using for the specific band are displayed. When an AP has been configured to use bonded channels, the word "Bonded" will appear below the channel number. See Figure 88.
 - ⑨ The Retries 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.
 - ⑩ If more than one band is being used, a second details box shows the data for the 5 GHz band.
 - ⑪ The Attributes section shows additional channel and network information.

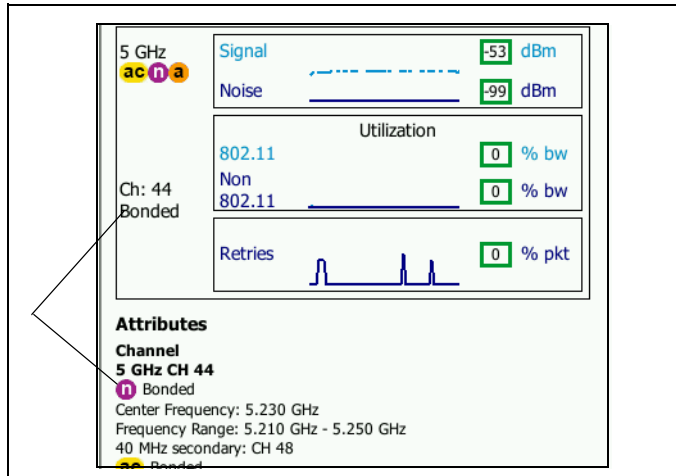








Figure 88. Bonded Channel AP Details

- The Channel section lists the center frequency, frequency range, channel width, and primary and secondary bonded channels for each band.
 - The Networks section (see Figure 87) shows each BSSID, SSID, and security protocol in use for each band.
- 12 Tap the information button to display quick tips about the screen.
 - 13 This is the date and time when the AP 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 Interferer Filter Button to show a summary of non-802.11 devices interfering with the AP. Tap the **SHOW ALL** button to show all interferers again.

- ⑩⑥ Tap the Channel Filter Button to show a summary of the channels the AP is using. Tap the SHOW ALL  button to show all channels again.
- ⑩⑦ Tap the Client Filter Button to show a summary of the clients associated with the AP. Tap the SHOW ALL  button to show all clients again.
- ⑩⑧ Tap the Network Filter Button to show a summary of the networks that are using the access point. Tap the SHOW ALL  button to show all networks again.
- ⑩⑨ 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.
- ⑩⑩ Indicates the presence of available Wired Analysis information.
- ⑩⑪ The signal strength icon provides a quick visual indication of the AP's signal strength as measured by the OneTouch analyzer. See [page 199](#) for a list of the thresholds that change the icon's appearance.
- ⑩⑫ This icon indicates the AP's security level (i.e. the security method the client uses to connect to the AP/network). See [page 199](#) 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.

When a specific network, AP, or client is selected, details are shown and related tools are available. The Wi-Fi **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 89)
- A graphical representation of client details and trended measurements
- Filter buttons that provide deeper analysis of each client's channel usage, access point association, network, and interferers

Each client is displayed with summary information on a button.

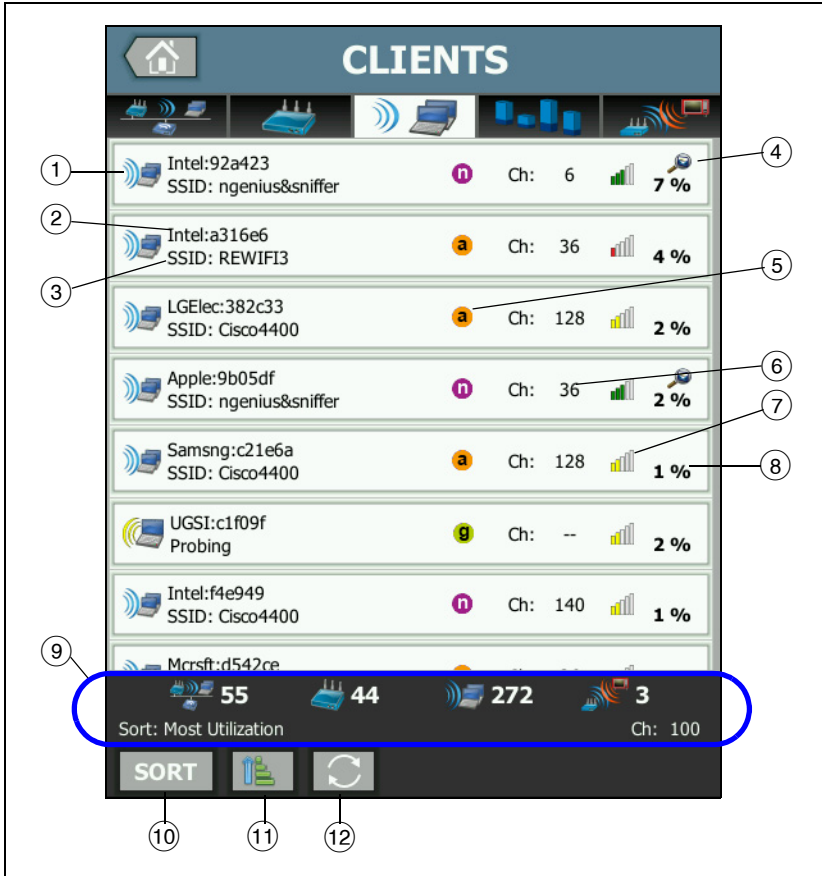




Figure 89. Client Analysis Tab

- 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 (SSID). 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 The presence of a Cross-link Discovery icon indicates device discovery during both Wi-Fi and Wired Analysis.
- ⑤ These icons indicate the 802.11 type, based on the highest connection rate observed by OneTouch. This provides visibility into a client's connection rate and a means to identify any slow connections (for example, an 802.11b client or a client too far away from the AP) that may be impacting network performance.

The 802.11 types in ascending order are 802.11b, 802.11g, 802.11a, 802.11n, and 802.11ac.




- ⑥ This is the channel the client is using.
- ⑦ The signal strength icon provides a quick visual indication of the client's signal strength as measured by the OneTouch analyzer. See [page 199](#) for a list of the thresholds that change the icon's appearance.
- ⑧ This changes based on the selected sort key. This shows the client's signal level (in dBm) as measured by the OneTouch analyzer, or it shows 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.
- ⑨ The status bar is displayed on all Wi-Fi ANALYSIS screens. It shows the number of networks (SSIDs), access points, clients, and interferers found.

This area also shows the current selected **Sort**: key on the left and channel numbers as they are scanned on the right.

- ⑩ 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)
- Cross-link Discovery (displays devices that were discovered during both, Wi-Fi and Wired Analysis).
- Channel number
- Utilization (the percentage of the AP's bandwidth that the client is using)
- 802.11 Type
- Retries (Retry Rate)
- SSID
- Access point
- Association (associated or probing state)

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

- 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 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.

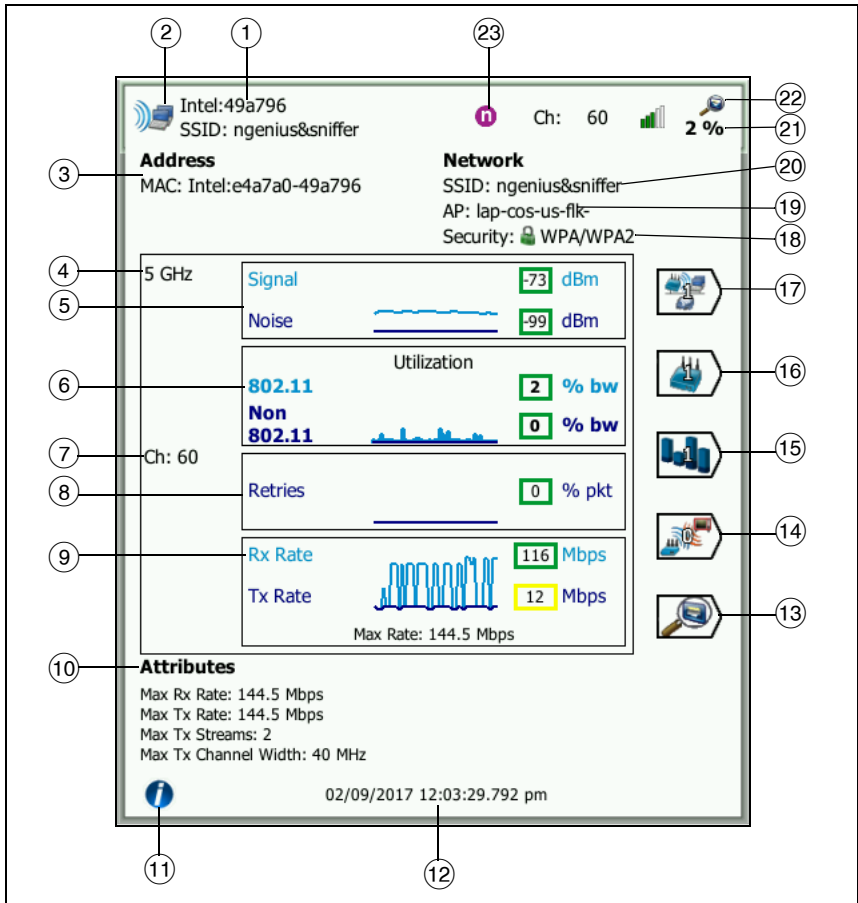




Figure 90. Associated Client Details

- 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 Band the client is using
- ⑤ 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.

- ⑥ The 802.11 utilization graph represents the Client's traffic on the respective AP and channel.




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.

- ⑦ Channel the client is using

- ⑧ The Retries 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.
- ⑨ The Frame Rate graph shows the receive (Rx) and transmit (Tx) rates. The scale for this graph is based on the Client'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.
- ⑩ The Attributes section on the client detail screen shows maximum connection rate (as observed by the OneTouch), number of streams, and maximum channel width for the client.
- ⑪ Tap the information button to display quick tips about the screen.
- ⑫ This is the time when the client 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 Interferer Filter Button to show a summary of non-802.11 devices interfering with the client. Tap the SHOW ALL  button to show all interferers again.

- ⑮ Tap the Channel Filter Button to show a summary of the channel the client is using. Tap the 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  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  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), and the type of security is indicated beside the icon. See [page 199](#) 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 The AP to which the client associated
- ⑳ The Network to which the client is connected
- ㉑ 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.
- ㉒ The presence of a Cross-link Discovery icon indicates device discovery during both Wi-Fi and Wired Analysis.
- ㉓ The Client's highest observed 802.11 media type.

Probing Client Details

Details for clients that are probing appear as shown below.

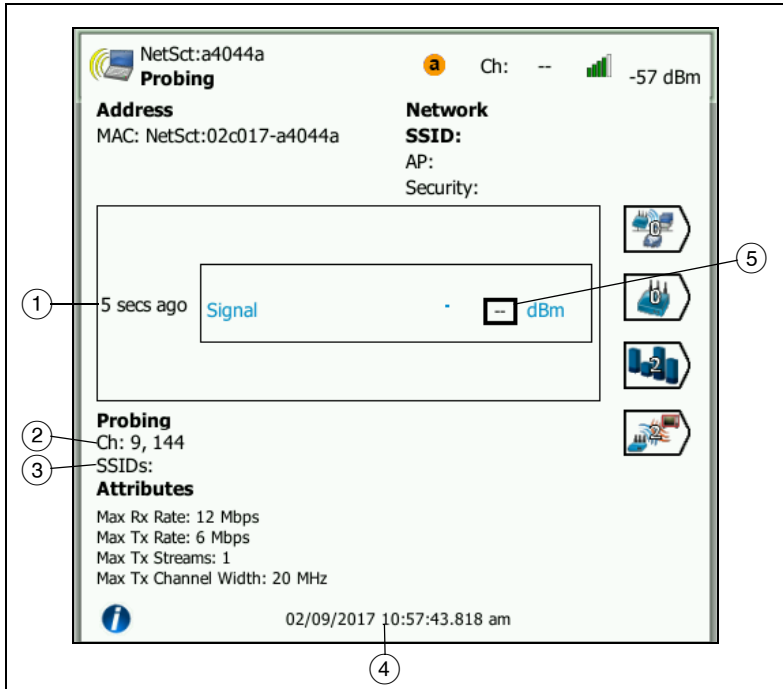



Figure 91. Probing Client Detail

- ① Time since the client last probed
- ② Channels on which the client is probing
- ③ SSIDs for which the client is probing
- ④ Time when the client was first discovered
- ⑤ Client's signal level as measured by the OneTouch analyzer. Dashes will be shown when the client is probing and a signal has not been detected.

Note

Connected Network Information (SSID, AP, and security) is not available for probing clients.

For an explanation of other client details, see Figure 90.

When a specific network, AP, or client is selected, details are shown and related tools are available. The Wi-Fi **TOOLS** button  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 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 92)
- 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, associated clients, and interferers

The top button on the Channel analysis tab provides a channel overview. Channel summary buttons appear below for each channel.

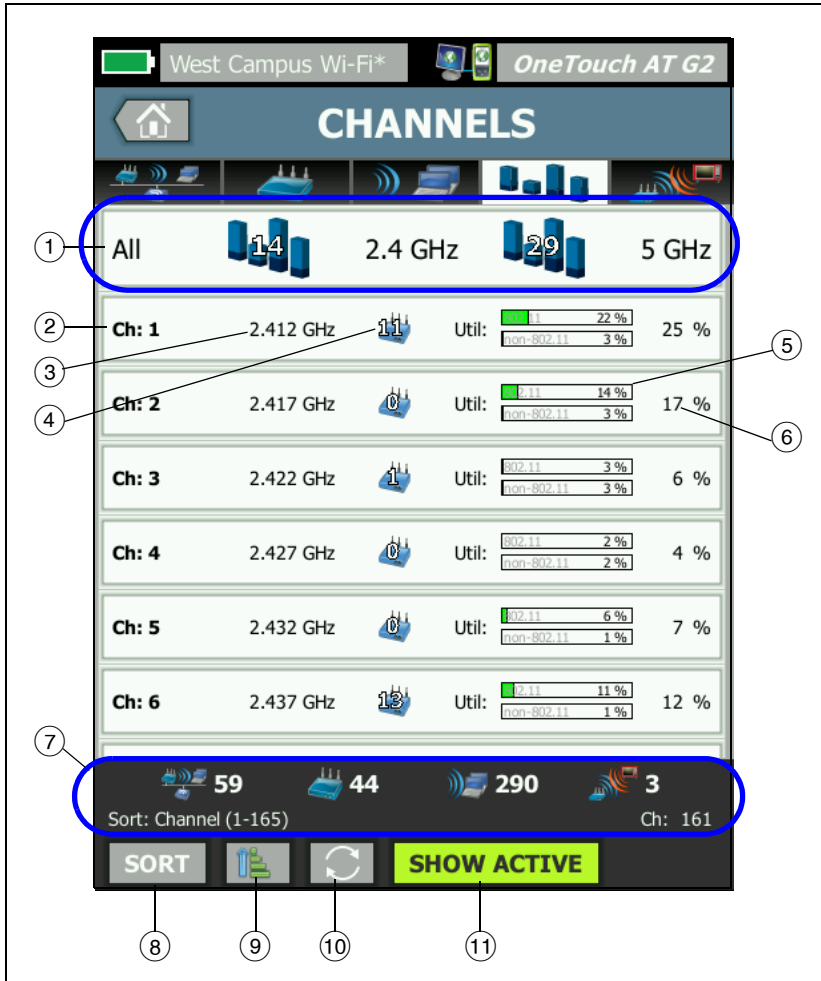


Figure 92. Channel Analysis Tab

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

- 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 shows 802.11 utilization and non-802.11 utilization, as noted by the gray watermark.
 - The bars are green if utilization is below the warning threshold.
 - The 802.11 utilization graph turns yellow if 802.11 utilization exceeds 40%.
 - The non-802.11 utilization graph turns yellow if non-802.11 utilization exceeds 20%.
- ⑥ This is the total percentage of channel utilization.
- ⑦ The status bar is displayed on all Wi-Fi ANALYSIS screens. It shows the number of networks (SSIDs), access points, clients, and interferers found.

This area also shows the current selected **Sort**: key on the left and channel numbers as they are scanned on the right.

- ⑧ The SORT button lets you sort the list of channels according to:
 - Channel number
 - Band
 - Total utilization
 - 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 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.
- ⑪ 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, and 802.11 traffic on all channels.

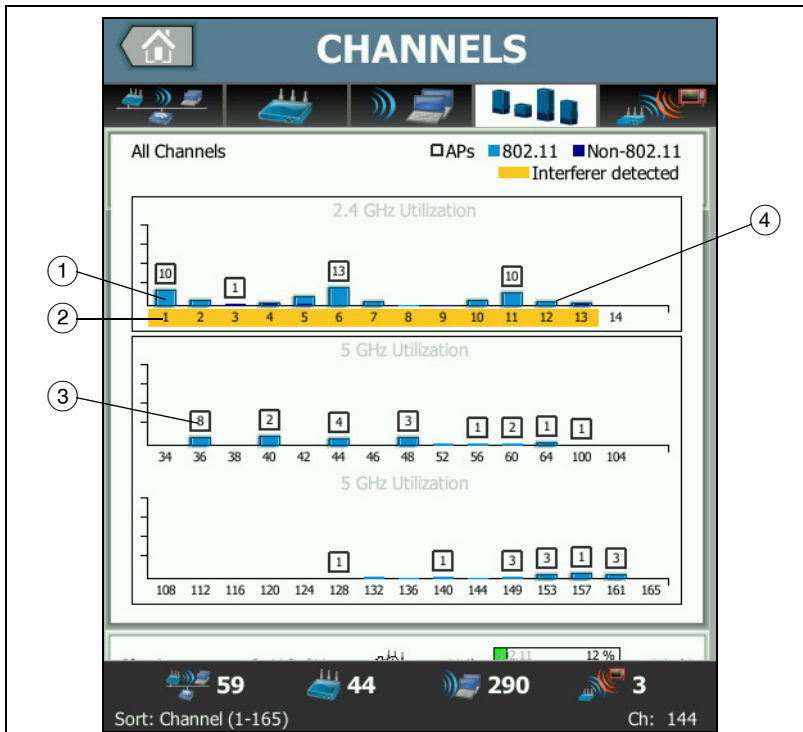


Figure 93. Channel Overview

- ① 802.11 utilization is shown as a light blue bar, and Non-802.11 utilization is a dark blue bar.
- ② Yellow highlighting indicates that an interferer is active on the highlighted channels.
- ③ The number of APs discovered on each channel is shown above the channel.
- ④ 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.

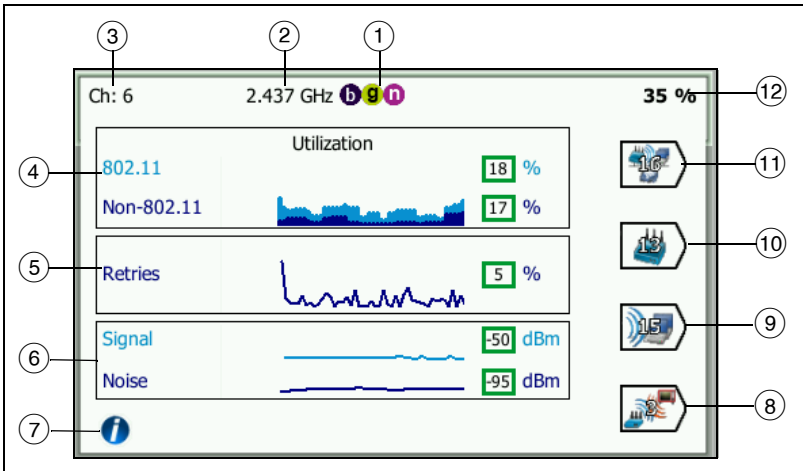


Figure 94. Wi-Fi Channel Details

- ① 802.11 media types supported in the respective band





- ② Channel frequency
- ③ Channel number
- ④ The utilization graph trends 802.11 utilization of the channel. The graph shows 802.11 utilization in light blue as a percentage of total bandwidth and non-802.11 utilization as dark blue. The graph's scale is 0% to 100%.
 - 802.11 utilization values less than 40% are shown in a green box.
 - Non-802.11 utilization values less than 20% are shown in a green box.
 - 802.11 utilization values greater than or equal to 40% are shown in a yellow box, indicating potentially excessive utilization.
 - Non-802.11 utilization values greater than or equal to 20% are shown in a yellow box, indicating potentially excessive interference.
- ⑤ The Retries graph gives you an indication of network coverage, congestion, and capacity problems.
- ⑥ 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.

- ⑦ 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.
- ⑧ Tap the Interferer Filter Button to show a summary of non-802.11 devices detected on the channel. Tap the SHOW ALL  button to show all interferers again.
- ⑨ Tap the Client Filter Button to show a summary of the clients discovered on the channel. Tap the SHOW ALL  button to show all clients again.
- ⑩ Tap the AP Filter Button to show a summary of the APs active on the channel. Tap the SHOW ALL  button to show all clients again.
- ⑪ Tap the Network Filter Button to show a summary of the networks utilizing the channel. Tap the SHOW ALL  button to show all clients again.
- ⑫ Total 802.11 utilization of the channel.

Interferer Analysis

The INTERFERER analysis tab provides:

- A sortable list of all discovered non-802.11 devices with summary information for each
- A graphical representation of interferer details and trended measurements
- Filter buttons that provide deeper analysis of each interferer's affected channels, access points, networks, and clients

Interferer summary buttons appear for each detected non-802.11 device.

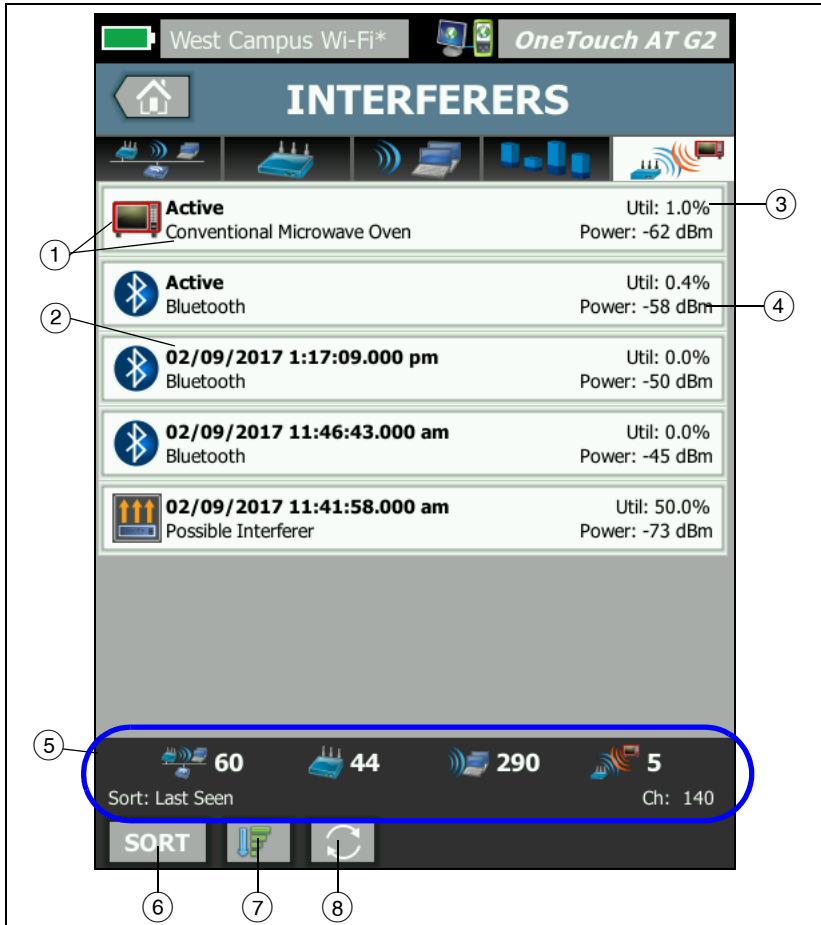


Figure 95. Interferer Analysis Tab

- ① The Interferer icon indicates the type of interfering device, along with the text description to the right of the icon. The interferer types that the OneTouch analyzer is able to identify include the following:
- Baby Monitor

- Bluetooth device
- Conventional Microwave Oven
- Cordless Phone
- Game Controller
- Jammer
- Motion Detector
- Wireless Video Camera
- Possible Interferer
- Unknown Interferer

② The time when the interferer was last seen by the OneTouch.

This field changes based on the sort key that you select. If you sort the interferer list by **Duration**, for example, this field shows the length of time the interferer was active in bold text. If you sort the list by **Most Affected Channel**, this field shows the most affected channel in bold, and so on for each sort option.

③ This shows the percentage of the channel's bandwidth that the interferer is using (utilization).

④ This shows the power level of the device's non-802.11 signal.

⑤ The status bar is displayed on all Wi-Fi ANALYSIS screens. It shows the number of networks (SSIDs), access points, clients, and interferers found.

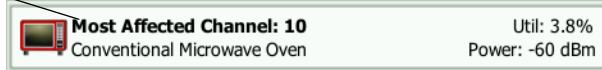
This area also shows the current selected **Sort**: key on the left and channel numbers as they are scanned on the right.

⑥ The SORT button lets you sort the list of interferers according to:




- Last Seen
- First Seen
- Duration
- Interferer Type
- Average Utilization

- Peak Utilization
- Average Power
- Peak Power
- Most Affected Channel

The sort key
is bold.



On interferer summary buttons, the sort key appears in bold text.

- ⑦ The Sort Order button determines whether the sorted results are shown in ascending  or descending  order.
- ⑧ The **REFRESH** button  clears all Wi-Fi analysis results and restarts Wi-Fi analysis.

To Show Interferer Details

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

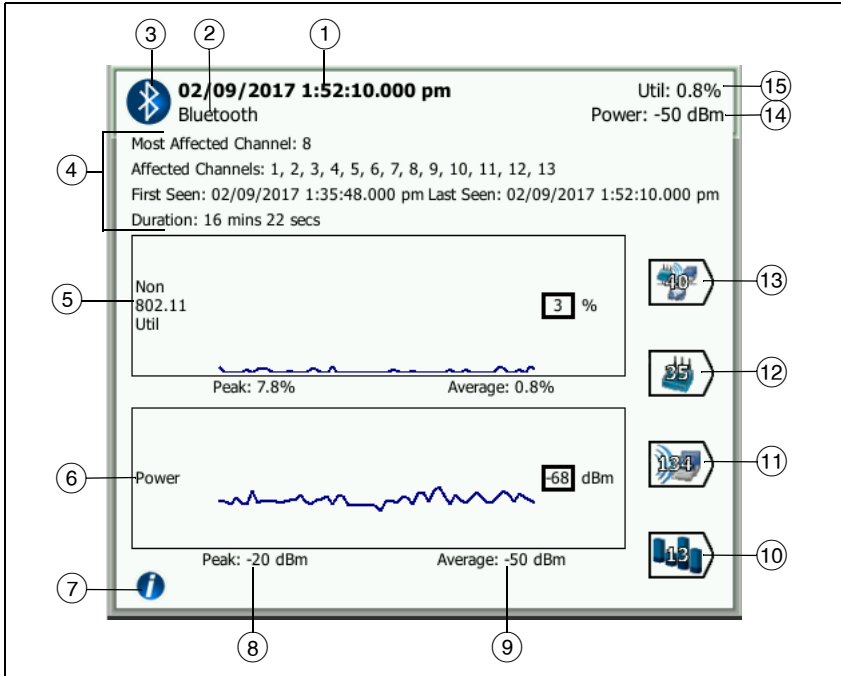






Figure 96. Interferer Details

- ① The time when the interferer was last seen by the OneTouch. If the interferer is currently being detected, this field shows **Active**.

This field changes based on the sort key that you select. If you sort the interferer list by **Duration**, for example, this field shows the length of time the interferer was active in bold text. If you sort the list by **Most Affected Channel**, this field shows the most affected channel in bold, and so on for each sort option.

- ② Name of the interferer type
- ③ Interferer type icon

- ④ Additional details, including most affected channel, all affected channels, time first seen, time last seen, and duration.
- ⑤ The Non-802.11 Utilization graph shows non-802.11 utilization over time as a dark blue line. The graph's scale is 0% to 100%. The **Peak:** and **Average:** utilization values are displayed below the utilization graph as percentages of total utilization.
- ⑥ The Power graph shows the power level of the interferer's non-802.11 signal over time.
- ⑦ Tap the information button to read about the impact and mitigation for the interferer type.
- ⑧ The Peak power level is displayed in dBm
- ⑨ The Average power level is displayed in dBm
- ⑩ Tap the Channel Filter Button to show a summary of channels affected by the interferer. Tap the SHOW ALL  button to show all interferers again.
- ⑪ Tap the Client Filter Button to show a summary of the clients affected by the interferer. Tap the SHOW ALL  button to show all interferers again.
- ⑫ Tap the AP Filter Button to show a summary of the APs affected by the interferer. Tap the SHOW ALL  button to show all interferers again.
- ⑬ Tap the Network Filter Button to show a summary of the networks affected by the interferer. Tap the SHOW ALL  button to show all interferers again.

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.



Figure 97. 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	Autho- rization	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.

Custom AP names up to 32 characters can be displayed by the OneTouch.

Note

You can also import an Authorization Control List (.acl) with the custom names and statuses of your APs. See "Save an Authorization File" on [page 237](#).

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 , 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 include the following:


 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.

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.


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.

After saving an ACL, you can export, import, and load it onto another OneTouch analyzer for use with a configured profile. You must **LOAD** a new ACL after importing it for the changes to take effect.

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.

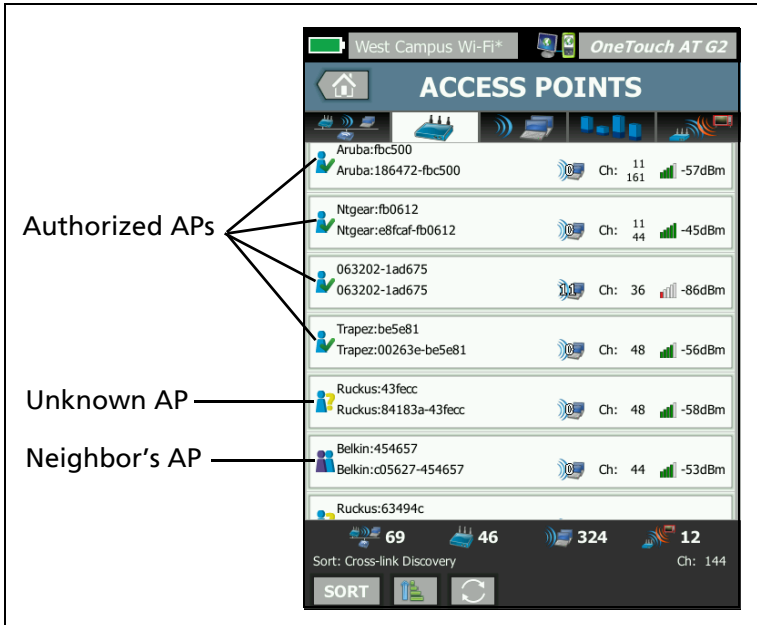



Figure 98. AP Authorization Status

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  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.

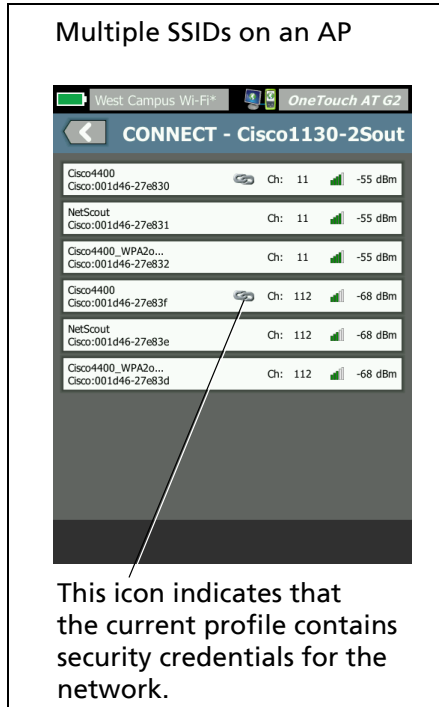


Figure 99. Multiple Choices for Connect tool

Note

The Wi-Fi ANALYSIS Network or AP connect tool operation is not affected by the Enable Connect option in Wi-Fi Test Settings in the TOOLS accessed from the Home screen. That setting is used for AutoTest only.

- 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.

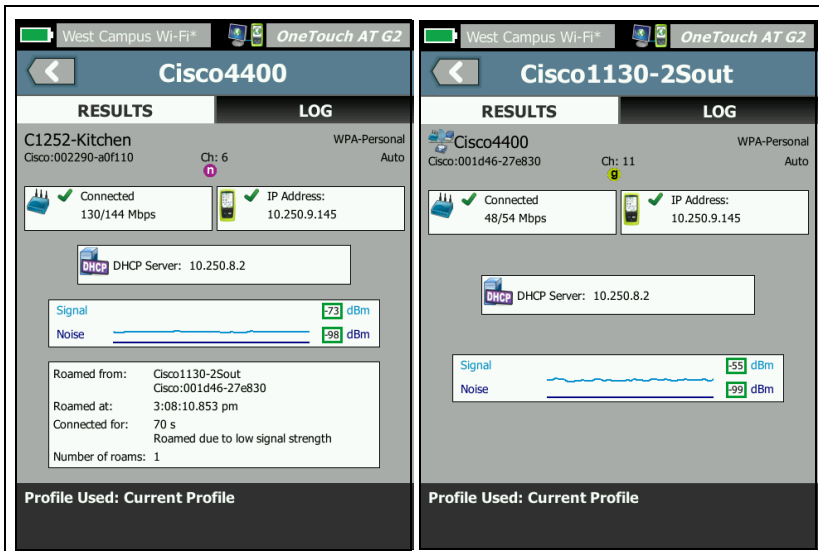


Figure 100. Network (left) and AP (right) Connect Tool Results

The network and AP connect RESULTS tabs show the network and AP, actual connection rate, the DHCP server's IP address, etc. If a static IP address is in use, the word "Static" appears next to the IP address label.

The signal and noise graph is explained on [page 209](#).

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.

For OneTouch AT G2 users: If you roam from one AP and connect to another AP, the reason for the roam appears here, under **Connected for**.

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.

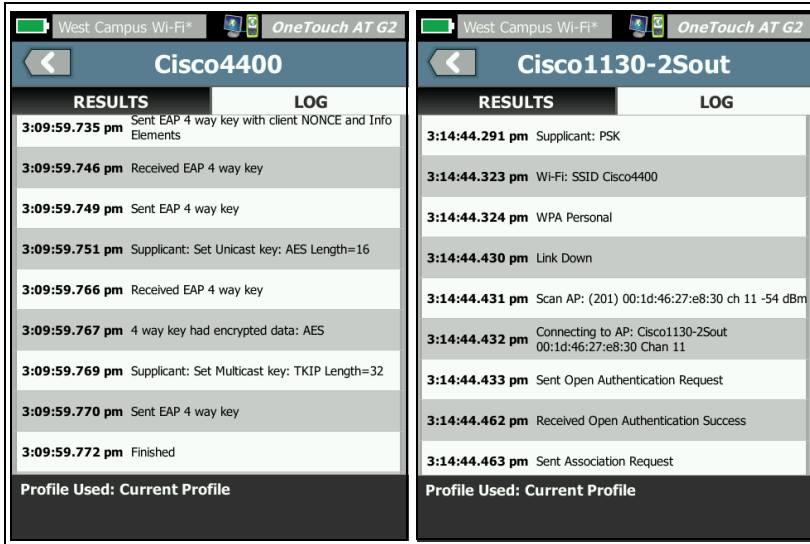


Figure 101. Network (left) and AP (right) Connection Logs

See also: “Wi-Fi Network Connect Test” on [page 86](#) and “Roaming Results Navigation Controls” on [page 90](#).

Locate Tool


You can use the Locate function to find APs, clients, or interferers.

You should use the directional antenna when performing a Locate task. See enterprise.netscout.com to purchase accessories for your OneTouch analyzer.

Note

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

To Locate a Wi-Fi Device

- 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 15](#)). The OneTouch analyzer automatically detects the presence of the antenna, and the external antenna icon  is displayed on the Locate RESULTS screen.

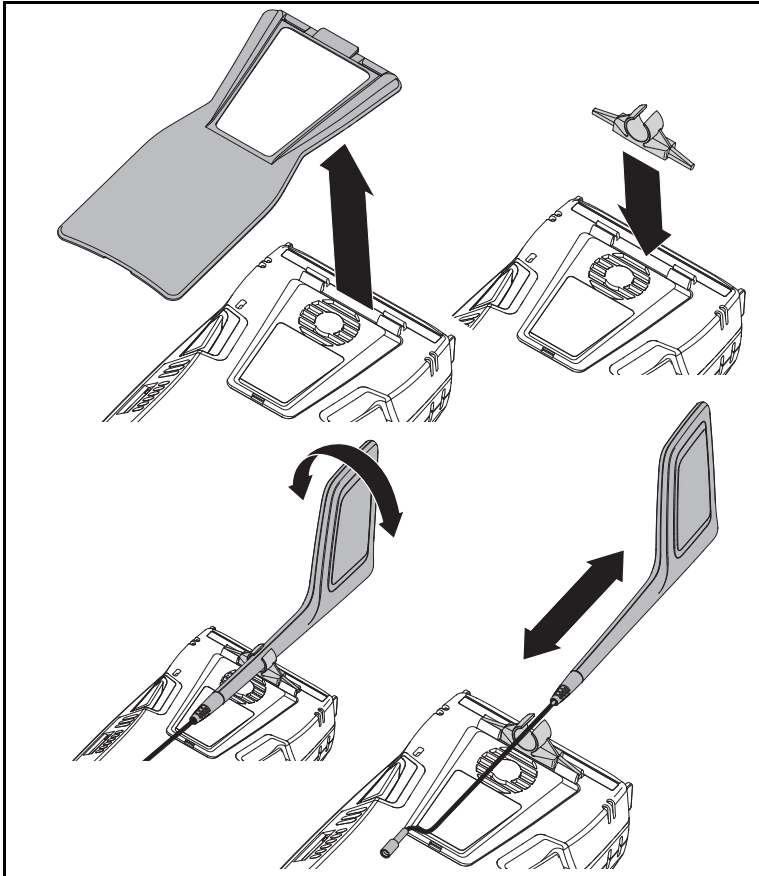


Figure 102. Directional Antenna Holder

- 5 Tap the **Locate** button from a Wi-Fi device's **TOOLS** screen to open the **LOCATE** screen.
- 6 View the signal strength graph and listen to the beeping sound to locate the device.

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

⚠ CAUTION

To avoid an accident, watch where you are going as you walk around locating the signal.

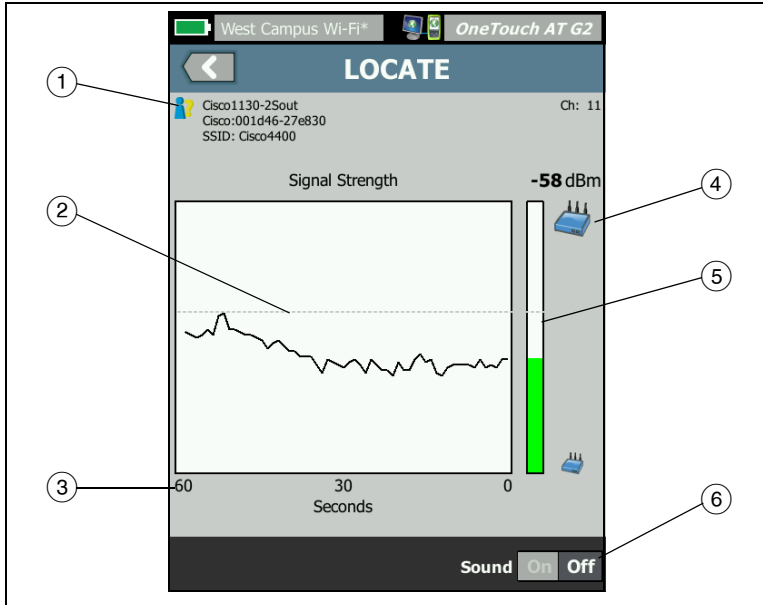


Figure 103. AP/Client LOCATE Screen

- 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 The graph shows one minute of signal data.
- 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 199](#). If the signal is lost, the bar turns gray.
- ⑥ You can switch off sound to silently locate APs or clients.

The **LOCATE** screen for Interferers is slightly different from the AP or Client **LOCATE** screen.

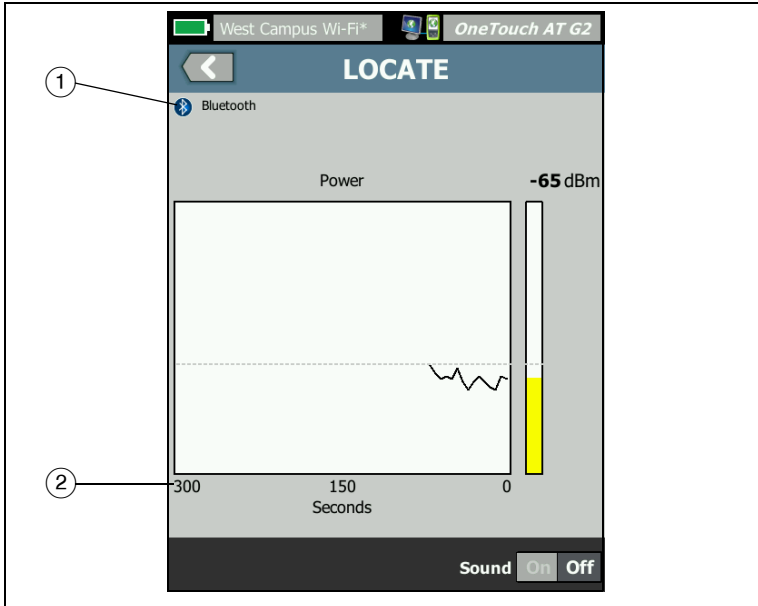



Figure 104. Interferer LOCATE Screen

- ① The Interferer icon indicates the type of interfering device, along with the text description to the right of the icon.
- ② The graph shows 5 minutes of signal data.

Note

If the Interferer you are locating becomes inactive, the screen pauses until the OneTouch detects the next active interferer of the same type and then resumes graphing its signal.

Chapter 9: Tools

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

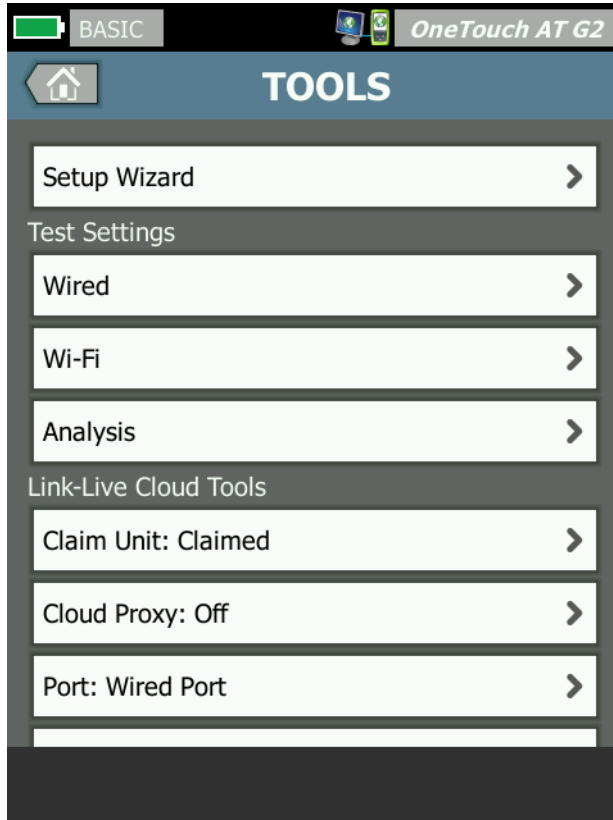


Figure 105. Tools Screen

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 169](#)

[“Slow Discovery” on page 169. Also included in this section:](#)

[“View or Change the analyzer’s MAC Addresses” on page 251](#)

Wired

On the HOME screen, tap **TOOLS** , then tap the **Wired** button to access the wired settings.

Enable/Disable Wired Analysis

The **Enable Wired** toggle button allows you to enable or disable the OneTouch’s wired analysis functions. Set to **Off** to use only the Wi-Fi connections and testing features.

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 76](#).

802.1X

Tap the **802.1X** button to open the SECURITY screen. Enable 802.1X authentication by setting **Enable** to **On**.

EAP - Select an EAP type that is appropriate for your authentication server.


If necessary for your selected EAP type, enter the **User** name (login name) and **Password**.

Alternate ID - The Alternate ID can be used with certain EAP methods to send an empty or anonymous identity in plain text while establishing a private connection. Once privacy is established, the 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.

To import a user authentication certificate:

- 1 Insert an SD card or USB drive with the required certificate into the correct port on your OneTouch.
- 2 Tap the **Certificate:** button and then the  (Manage) button to open the MANAGE CERTIFICATES screen.
- 3 Tap IMPORT to open the IMPORT CERTIFICATE screen.
- 4 Select the storage location where the certificate is saved.
- 5 Select the certificate file, and then tap **OK**.

For more information on importing and exporting files, see “Managing Files” on [page 341](#).

Address

The IPv6 option on the ADDRESS screen determines whether the IPv6 columns are shown on user test RESULTS screens. The wired IPv4 test results column is always displayed. IPv6 results are displayed if IPv6 is enabled as described below. The IPv4, IPv6, and

MAC Address options listed below apply to 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 48](#).

See “Wi-Fi TOOLS” on [page 234](#).

Analysis

See “SNMP” on [page 169](#), and “Slow Discovery” on [page 169](#).

This button is not available if Enable Wired is Off.

Link-Live Cloud Tools

The Link-Live Cloud tools are for interacting with the Link-Live Cloud Service.

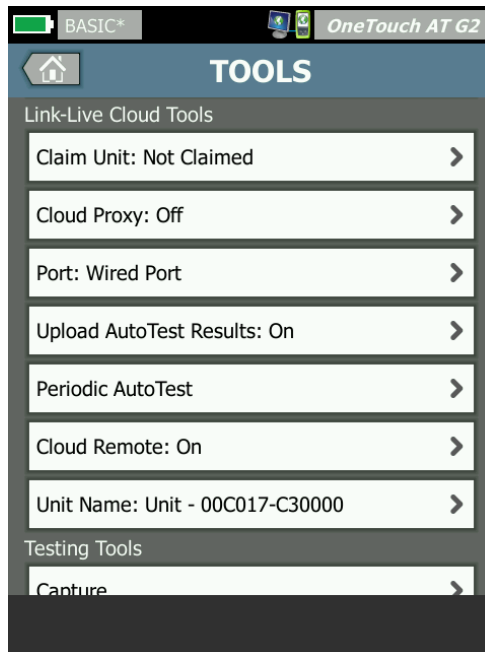


Figure 106. Link-Live Cloud Tools

Claim Unit:

You must *claim* your OneTouch AT analyzer before you can view its test results in the Link-Live Cloud. For additional information see “Claiming Your Unit,” beginning on [page 360](#).

Cloud Proxy:

By default this setting is off. If you choose to enable it, additional input options will be shown: Proxy Address, Proxy Type, and Proxy Port.

Port:

By default, the OneTouch automatically detects and uses an appropriate port. If needed, you can specify the Management Port, the Wired Port, or the Wi-Fi Port to communicate with the Cloud Service and upload test results and reports.

Note

You must have an active connection to the Management Port when claiming your unit or uploading screenshots to the Link-Live Cloud Service. Test results and reports will upload via any available port.


Upload AutoTest Results:

Turn this setting off if you do not want your OneTouch to upload AutoTest results to Link-Live Cloud Service.

Periodic AutoTest

When the analyzer is in Periodic AutoTest mode, the OneTouch runs AutoTests at specified intervals and sends the results to Link-Live so that you can view the results over time. The OneTouch AT unit must be claimed before any Periodic AutoTesting can occur, and Periodic AutoTesting must be configured to allow the OneTouch AT's test results to be sent to the Link-Live Cloud.

To enable Periodic AutoTest:

- 1 Select **TOOLS**  from the HOME screen.
- 2 Under **Link-Live Cloud Tools**, select **Periodic AutoTest**.
- 3 Configure the following:

Duration - The length of time during which test results will be

sent to the Link-Live Cloud. The duration can be set to Unlimited Duration, 2, 5, 10, and 30 minutes, or 1 hour, 2 hours, 3 hours, 4 hours, 5 hours, 6 hrs, 8 hrs, and 12 hrs, or 1 day, 2 days, 3 days, 4 days, 5 days, or 1 week, or 2 weeks.

Interval - This is the amount of time between sent test results to the Link-Live Cloud over a selected time duration.

Comment - This entry will appear beneath the Periodic Auto-Test results in Link-Live Cloud Service. Use this feature to annotate your Periodic AutoTest session.

Backlight Timeout - This feature controls how long the One-Touch screen's backlight stays illuminated while Periodic Auto-Testing is ongoing.

Cloud Remote:

Enable this option when you want to allow the claimed unit to be accessed remotely from the Link-Live Cloud. See [page 364](#).

Unit Name:

You can give your OneTouch AT a descriptive name to make it easier to identify when working in the Link-Live Cloud. See [page 360](#).

Testing Tools

The following testing tools are available on the TOOLS screen.

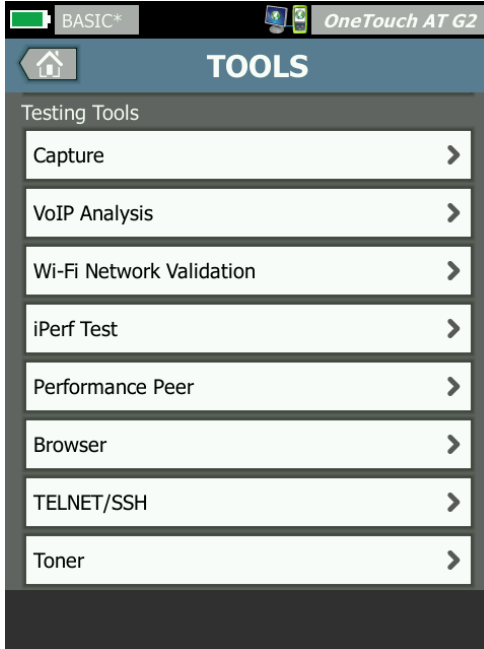


Figure 107. Testing Tools

Capture

See Chapter 10, "[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 in-line 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.

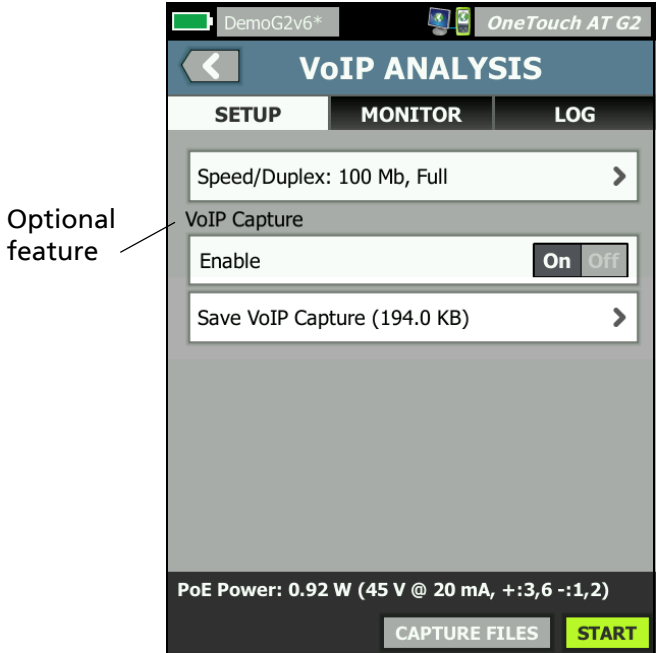


Figure 108. The VoIP Analysis Configuration Screen, SETUP Tab

- 5 Tap the **Speed/Duplex** button. Select the phone's link speed and duplex mode, or select the **Auto** option to allow the OneTouch to link on both ports at the fastest common speed and duplex detected.
- 6 Optional: Enable VoIP Analysis packet capture. See [page 262](#).

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

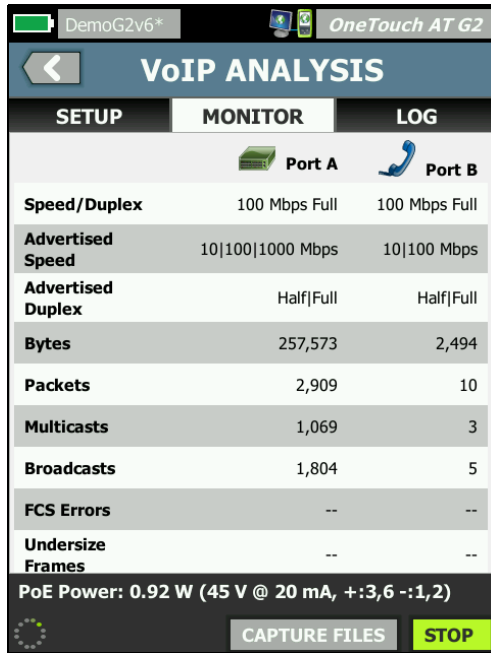



Figure 109. The VoIP Analysis Results Screen, MONITOR Tab

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 265](#).

VoIP ANALYSIS Screen, LOG Tab

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

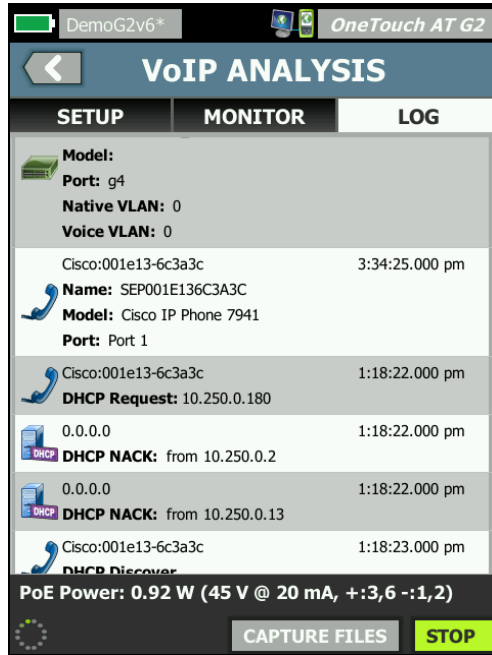


Figure 110. The VoIP Analysis Results Screen, LOG Tab

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 server



VoIP call manager



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 ClearSight Analyzer software or other protocol analysis software. Use VoIP capture for saving VoIP

traffic. Use packet capture (see Chapter 10: "Packet Capture," beginning on [page 319](#)) to capture higher volume traffic.

- 1 Follow steps 1 through 5, beginning on [page 257](#).
- 2 On the VoIP Capture Enable button, select **On**.

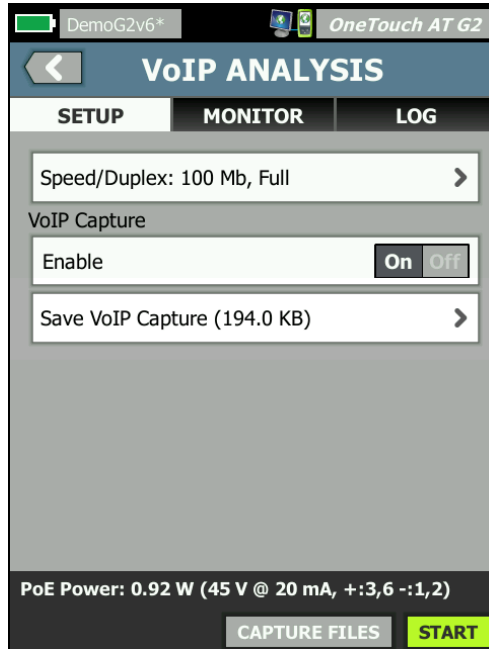



Figure 111. The VoIP Analysis Configuration Screen

- 3 Tap the **START** button .
- 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.

- When you determine that the packets of interest have been exchanged, tap the STOP button to stop the test and the capture. The VoIP ANALYSIS configuration screen is displayed.

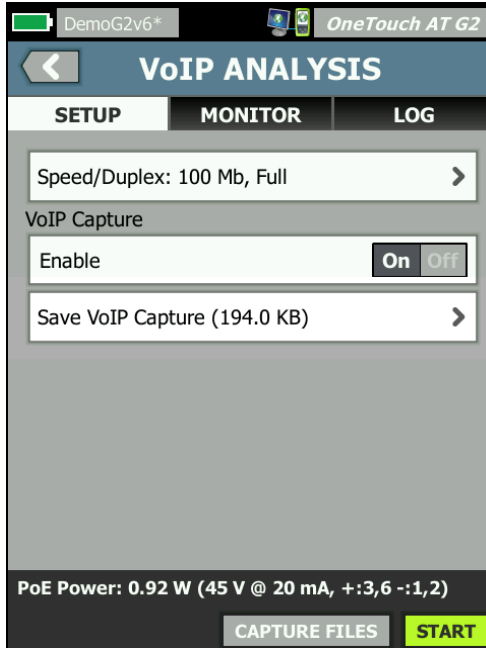


Figure 112. The VoIP Analysis - Save VoIP Capture

The **Save VoIP Capture** button is displayed, indicating that packets were captured and they can be saved to a file.

- 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.

- 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 .

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 341](#).

Analyzing Capture Files

You can use 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.

Wi-Fi Network Validation

The Wi-Fi Network Validation tool provides a way for you to verify and report on network availability, coverage, and performance at your sites by running Wi-Fi Performance Tests on your APs.


A Peer or Reflector device is required to perform Wi-Fi Network Validation Testing. See [“Wi-Fi Performance Test”](#) in Chapter 5: “User Tests,” beginning on [page 103](#) for more detail on configuring Wi-Fi Performance Tests and how they work.

To perform Wi-Fi Network Validation, you must select a network SSID to test, set up your devices for Wi-Fi Performance Testing, and save a descriptive name for the physical locations where you plan to test Wi-Fi availability.

Note

The SSID(s) you chose for Wi-Fi Network Validation must already be configured with the proper credentials in a profile saved on the OneTouch. See “Wi-Fi” on [page 252](#).

To Configure Wi-Fi Network Validation

- 1 On the HOME screen, tap **TOOLS** .
- 2 In the **Testing Tools** section, tap the **Wi-Fi Network Validation** button.

The Wi-Fi Network Validation screen is displayed.

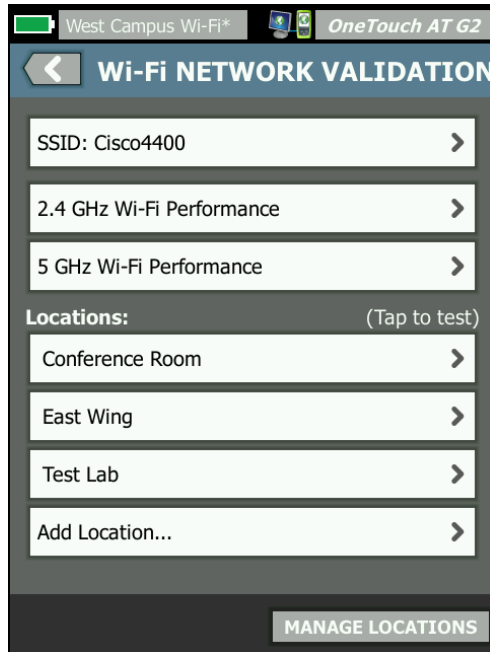


Figure 113. The Wi-Fi Network Validation Screen

- 3 Tap **SSID:** to select a network for testing. In the image above, the "Cisco4400" SSID has been selected.

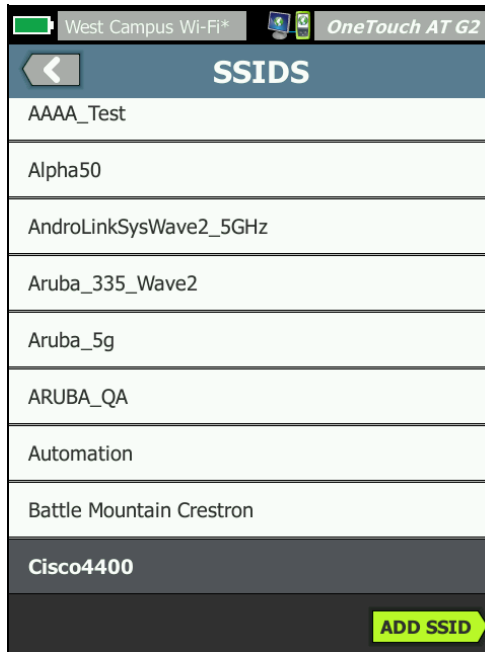


Figure 114. Wi-Fi Network Validation SSID Selection Screen

- 4 Tap the network name for the network you want to test, or tap **ADD SSID** to type in the SSID name.

Once added, your chosen SSID is shown on the Wi-Fi Network Validation screen (Figure 113).

- 5 Tap **2.4 GHz Wi-Fi Performance** and/or **5 GHz Wi-Fi Performance** to configure the settings for each type of test. These will be the default settings used for your Wi-Fi Network Validation testing.

For instructions on setting up Wi-Fi Performance Tests, see [“Wi-Fi Performance Test”](#) in Chapter 5: “User Tests,” beginning on [page 103](#). Note that the “This OneTouch” performance test type is not available for Wi-Fi Network Validation; you must have a Peer or Reflector device.

To further customize performance test settings for individual BSSIDs, see “To Run Wi-Fi Network Validation Tests” on [page 272](#).

- 6 Next, tap the **Add Location...** button to save descriptive names for each location from which you plan to run Wi-Fi Network Validation testing.
- 7 Use the keyboard to type in a meaningful description for each location, which could include GPS coordinates or physical landmarks to indicate an exact location.
- 8 When you finish entering a descriptive Location name, tap **DONE**.
- 9 To rename or delete Locations you have saved, tap the **MANAGE LOCATIONS** button at the bottom right of the Wi-Fi NETWORK VALIDATION screen.

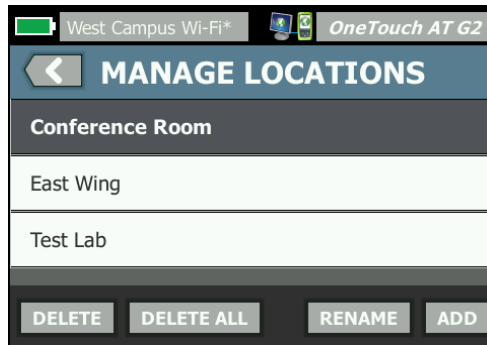



Figure 115. Manage Locations for Wi-Fi Network Validation

- To rename or delete a location, select the location’s name, and then tap the button for the action you want to complete.
- Tap ADD to enter additional locations from the MANAGE LOCATIONS Screen.
- Tap the Back button  to return to the Wi-Fi Network Validation screen.

To Run Wi-Fi Network Validation Tests

- 1 To begin Wi-Fi Network Validation testing, you must physically go to your target test location, and tap the Location on the Wi-Fi NETWORK VALIDATION screen (see [Figure 113](#)).

Note

If you are not performing Wi-Fi Validation Testing from the physical location where you wish to test Wi-Fi coverage, your results will reflect where the OneTouch is currently located, not your saved location.

The OneTouch scans the network for associated BSSIDs and compiles a list.

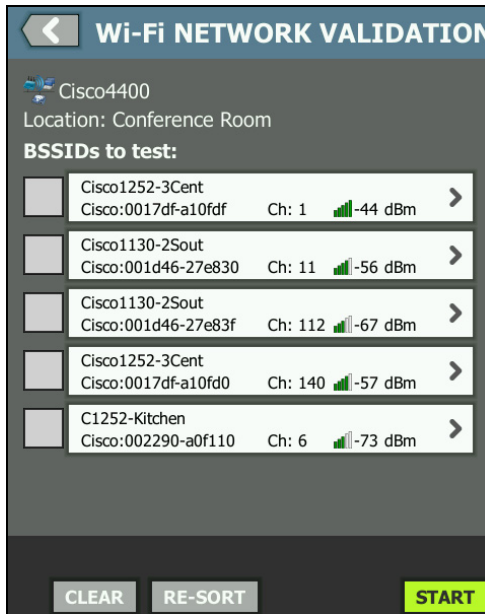



Figure 116. Discovered BSSIDs for Wi-Fi Network Validation

- 2 The BSSID list updates as BSSIDs are identified. Once BSSID discovery is complete, you can tap the **RE-SORT** button to update the list, moving the BSSIDs with the strongest signal strength to the top of the list. Tap **CLEAR** to start the discovery scan for BSSIDs again.
- 3 Check the boxes next to the BSSIDs you want to test during Wi-Fi Network Validation.
- 4 Optionally, tap any BSSID button to customize the network validation test settings on the SETUP tab for that individual BSSID. See [“Wi-Fi Performance Setup Tab” on page 146](#).
- 5 To run the Wi-Fi Performance tests for all BSSIDs you have selected on the Wi-Fi NETWORK VALIDATION screen, tap the **START** button .

To View Wi-Fi Network Validation Results

After you tap START, the OneTouch begins running the Wi-Fi Performance Test on each selected BSSID sequentially.

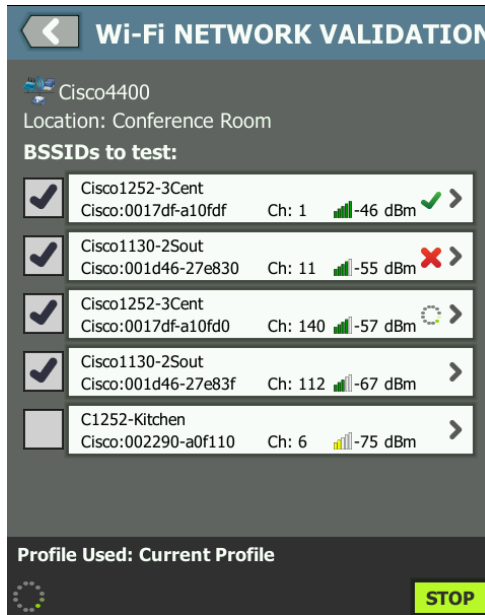





Figure 117. Wi-Fi Network Validation in Progress

At the bottom-left corner of the screen and next to each tested BSSID, 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.

At any time, tap a BSSID button on your checklist to go to its test SETUP, RESULTS, and LOG tabs.

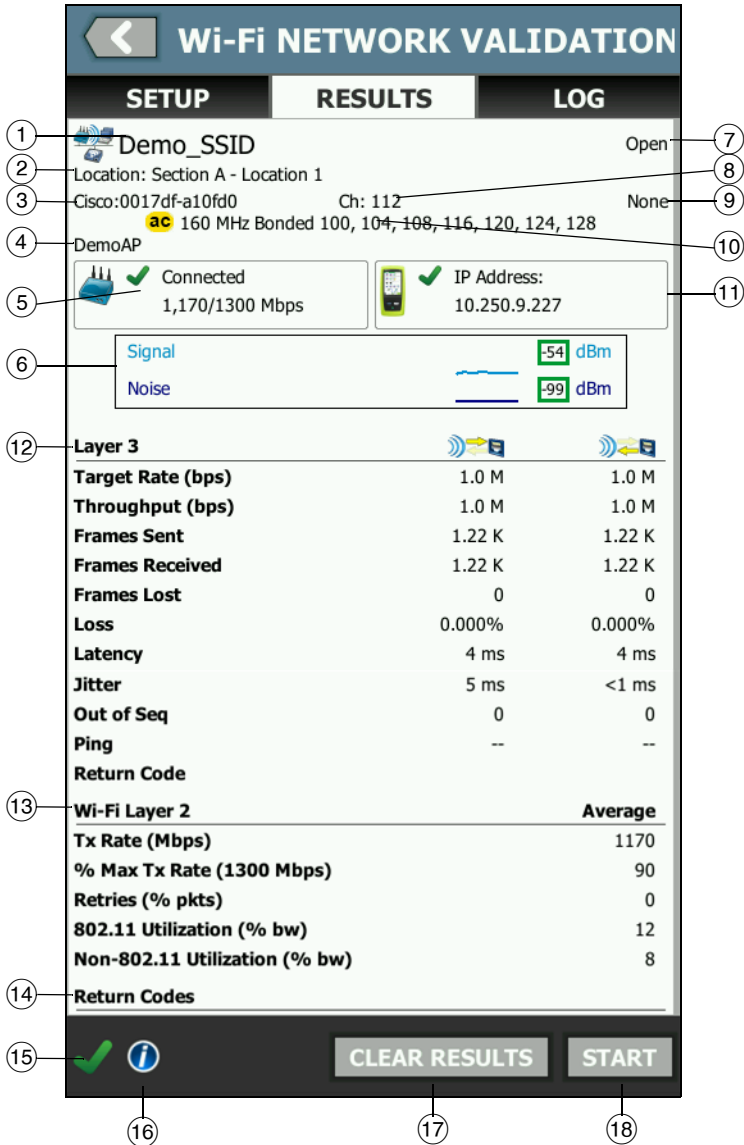


Figure 118. Wi-Fi Network Validation Results Tab

The Wi-Fi NETWORK VALIDATION RESULTS tab displays Signal and Noise measurements as well as Layer 3 and Wi-Fi Layer 2 test metrics.

- ① SSID - The name of the network on which the Wi-Fi connection was established during the test.
- ② **Location:** This is the location name from which you should be running this test.
- ③ BSSID - This row shows the Access Point manufacturer and BSSID.
- ④ AP Name - This is the AP's name.
- ⑤ Connection Status - This shows whether the OneTouch was able to establish a connection with the AP, and if connected, indicates the current and maximum transmit rates, as current/max Mbps.
- ⑥ The **Signal and Noise** graph gives you an indication of the access point's coverage and the signal quality for the duration of the performance test.






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 This is the security type used when connecting to the BSSID.
 - ⑧ This is the channel on which the BSSID is operating.

- ⑨ This is the encryption type used when connecting to the BSSID (for example: None, AES, TKIP, WEP-64, WEP-128, WEP, or Auto).
- ⑩ This displays 802.11 information for the current Wi-Fi connection.
- ⑪ **IP Address:** This is the OneTouch AT's IP address.
- ⑫ **Layer 3 - Stream direction** is indicated by the icon at the top of the column.
 - **Target Rate (bps)** is the requested bit rate from the SETUP tab.
 - **Throughput (bps)** is the measured bit rate based on frames sent and the actual number of frames received.
 - **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.
 - **Latency** is the average one-way latency for 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.

- ⑬ **Wi-Fi Layer 2** - Shows average measurements:
- **Tx Rate (Mbps)** - The average transmission rate is shown in Mbps or Kbps.
 - **% Max Tx Rate (Mbps)** - The percentage of the maximum transmission rate is shown in Mbps or Kbps. When the average rate is less than 30% of the maximum rate, a warning icon  is displayed.
 - **Retries (% pkts)**- A warning icon  is displayed when the average retry rate exceeds 40% of total packets.
 - **802.11 Utilization (% bw)** - 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.
 - **(OneTouch AT G2 only) Non-802.11 Utilization (% bw)** - Non-802.11 utilization is reported in terms of the percentage of bandwidth usage on the connected channel.
- ⑭ **Return Codes** specify the end-of-test status or an error condition if encountered.
- ⑮ 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.
- ⑯ Tap the information button to display quick tips about the screen.
- ⑰ Tap **CLEAR RESULTS** to clear all data on the screen.
- ⑱ Tap the **START** button to re-run the test for the current BSSID only.

To Save Wi-Fi Network Validation Results

You can save the results of Wi-Fi Network Validation testing for multiple locations and BSSIDs to a Report and send the Report to the Link-Live Cloud Service.

Note

If you change the SSID: on the Wi-Fi NETWORK VALIDATION screen, all previous Wi-Fi Network Validation results are cleared and discarded. Save a Report with your results before switching to a new network/SSID. A pop-up notification will warn you before the analyzer discards the previous results.

Tap the OneTouch AT shortcut button at the top right of the analyzer screen to access the SAVE REPORT button and screen.

See “Reports” on [page 300](#) in this chapter for details on how to save Report options.

iPerf Test

The iPerf Test is a standardized network performance tool used to measure UDP or TCP capacity and throughput. The OneTouch can perform iPerf testing using either a NETSCOUT Test Accessory endpoint or iPerf3 software installed on a PC or other device as the endpoint.




OneTouch can automatically discover, and use as endpoints, Test Accessories that are claimed to the same organization as your OneTouch unit on Link-Live Cloud Service. See “Link-Live Cloud Service” on [page 359](#) and your Test Accessory User Guide for more information.

To use an iPerf server installed on a PC or other device as the endpoint, iPerf version 3.0 or higher is required. You can download it at this URL: <https://iperf.fr>

OneTouch G2 can perform either a Wired or Wi-Fi iPerf test. To perform iPerf Performance Testing, your OneTouch must be connected to an active wired or Wi-Fi network.

To Configure an iPerf Test

- 1 On the HOME screen, tap **TOOLS** .
- 2 In the **Testing Tools** section, tap the **iPerf Test** button.

The iPerf Test screen is displayed.

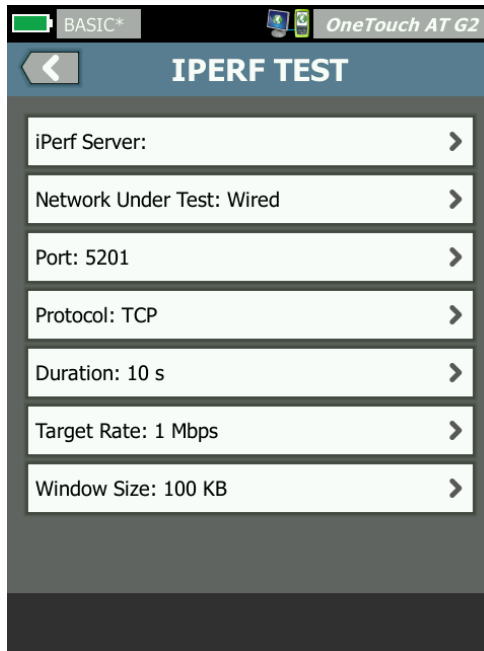


Figure 119. iPerf Test Setup Screen

- 3 Touch the **iPerf Server:** button to open the iPerf Server screen.



Figure 120. iPerf Server Screen

- 4 Your iPerf server can be either a Test Accessory or iPerf software installed on another device. Select the appropriate iPerf test endpoint using one of the following methods:
 - Touch the **iPerf Server:** button on the IPERF SERVER screen to manually enter your iPerf server's IPv4 address or URL using the virtual keyboard. Touch DONE to save your entry.
 - If it is claimed to Link-Live, OneTouch automatically queries Link-Live for any claimed Test Accessories in the same organization and displays them in the **Available iPerf Remotes** list. Touch the **QUERY IPERFS** button to re-query Link-Live for Test Accessories. Select a discovered Test Accessory from the list to use it as your iPerf Server.

Note

You must have a NETSCOUT Test Accessory claimed to the same organization as your OneTouch unit for your OneTouch to be able to discover the Test Accessory for iPerf testing.

Additionally, your OneTouch must be connected to a network via the Management Port to query Link-Live. If using Wi-Fi, you can use a Wi-Fi dongle connected to the Management Port.

Once selected, the iPerf Server software's or Test Accessory's address displays in the top field on the iPerf Test screen.

- 5 Tap **Network Under Test**: to select either your **Wired** or **Wi-Fi** network connection for testing.

Note

*If you have Wired or Wi-Fi disabled on the currently loaded profile, the **Network Under Test** button will not be visible.*

- 6 If needed, tap **Port** to enter a port number other than the default 5201.

Note

If you change the default Port number on the OneTouch, you must also change the Port number in the iPerf server's settings to match.

- 7 Choose a **Protocol** to test, either **TCP** or **UDP**.

The test parameter options change depending on the selected Protocol. Figure 119 shows the TCP parameters and Figure 121 shows UDP test parameters.

Protocol: UDP	>
Duration: 10 s	>
Target Rate: 1 Mbps	>
Loss Limit: 1%	>
Jitter: 50 ms	>

Figure 121. UDP Protocol Parameters

- 8 Adjust the iPerf test **Duration**, **Target Rate**, **Window Size**, **Loss Limit**, and/or **Jitter** as needed for your testing purposes.

To Run an iPerf Test

- 1 To begin the test, tap the **START** button at the bottom of the iPerf Test screen.

If you are performing a Wired test, the iPerf test begins, and the Wired results screen appears.

- 2 If you are testing over a Wi-Fi network, select a network from the discovered list for testing, or touch **ADD SSID** to enter a new network name.

Note

The SSID you choose for iPerf testing must already be configured with the proper credentials in a profile saved on the OneTouch. See "Wi-Fi" on [page 252](#).

Once an SSID is selected, the OneTouch populates **BSSIDs to test** from the chosen network.



Figure 122. Select BSSIDs for iPerf Test

- 3 To test only one BSSID, touch its row to open the results screen (Figure 125), and then touch the **START** button.
- 4 To test more than one BSSID:
 - Select the BSSIDs you want to test from the discovered list by touching the checkbox to the left of its row.
 - To begin testing one or more BSSIDs, tap the **START** button at the bottom of the IPERF screen.
 - To view individual results, touch a BSSID's row.

The Wi-Fi iPerf results screen appears and begins populating measurements.

To View iPerf Test Results

The results screen header displays the IP address of the selected iPerf server.

Specific test results vary depending on the Protocol (TCP or UDP) being tested.

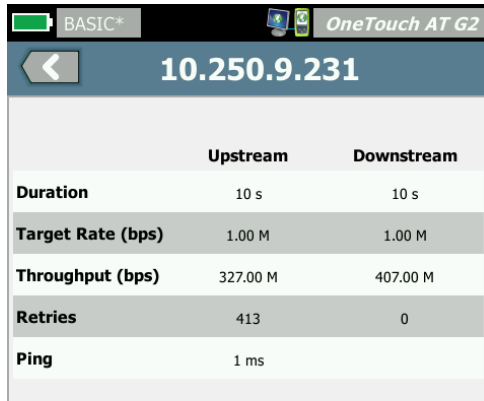
At the bottom-left corner of the screen, an icon indicates the test's status:

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

An error message indicates the reason for test failure.

Wired iPerf Test Results

TCP Protocol Test Results



	Upstream	Downstream
Duration	10 s	10 s
Target Rate (bps)	1.00 M	1.00 M
Throughput (bps)	327.00 M	407.00 M
Retries	413	0
Ping	1 ms	

Figure 123. Wired iPerf TCP Test Results

Duration is the length of time the test ran.

Target Rate (bps), for the TCP protocol, is the pass/fail threshold for the test, as set on the iPerf Test setup screen.

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

Retries (TCP Protocol only) is the number of retransmitted TCP segments.

Ping shows the Ping response time from the iPerf server.

Note

If the Ping portion of the test fails, the entire iPerf test will fail.

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

UDP Protocol Results



	Upstream	Downstream
Duration	10 s	10 s
Target Rate (bps)	1.00 M	1.00 M
Throughput (bps)	1.00 M	1.00 M
Frames Sent	862	862
Frames Recvd	862	862
Frames Lost	0	0
Jitter	457.00 us	57.00 us
Ping	<1 ms	

Figure 124. Wired iPerf UDP Test Results

Duration is the length of time the test ran.

Target Rate (bps) is the requested bit rate from the iPerf Test setup screen.

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

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

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

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

Jitter is the average frame delay variation.

Ping shows the Ping response time from the iPerf server.

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

Wi-Fi iPerf Test Results

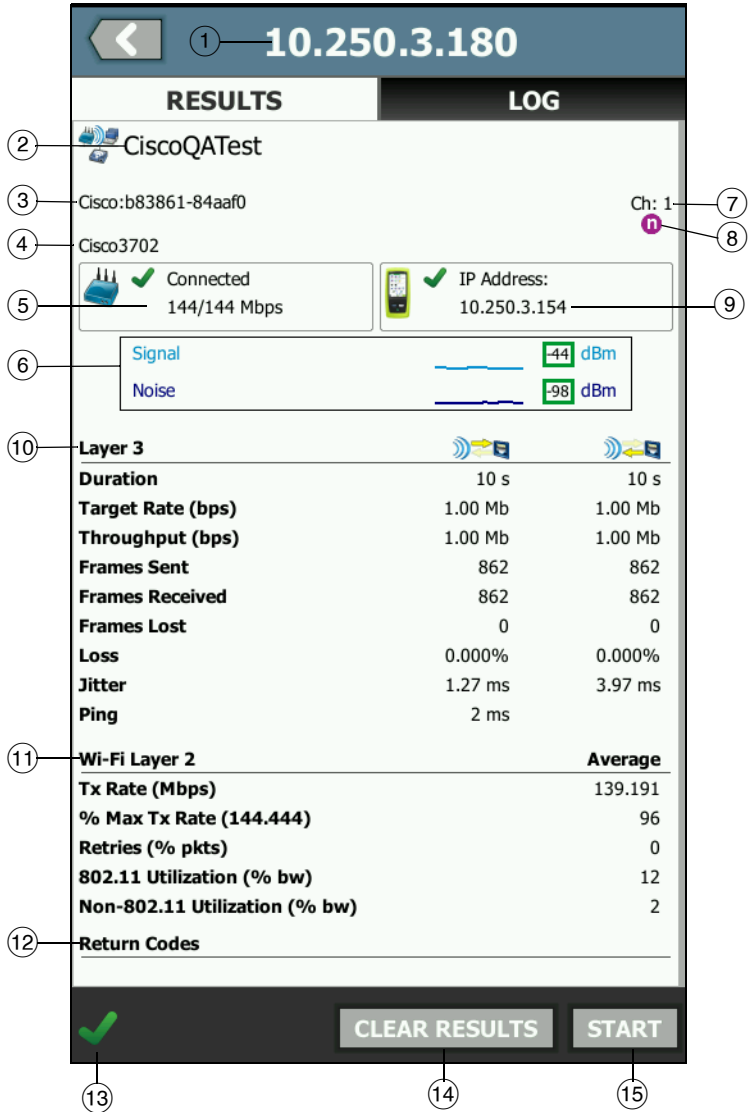


Figure 125. Wi-Fi iPerf UDP Test Results

- ① The IP address of the selected iPerf server.
- ② SSID - The name of the network on which the Wi-Fi connection was established during the test.
- ③ BSSID - This row shows the Access Point manufacturer and BSSID.
- ④ AP Name - This is the AP's name.
- ⑤ Connection Status - This shows whether the OneTouch was able to establish a connection with the AP, and if connected, indicates the current and maximum transmit rates, as current/max Mbps.
- ⑥ The **Signal** and **Noise** graph gives you an indication of the access point's coverage and the signal quality for the duration of the performance test.

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 This is the channel on which the BSSID is operating.
- ⑧ This row displays 802.11 information for the current Wi-Fi connection.
- ⑨ **IP Address:** This is the OneTouch AT's IP address.
- ⑩ **Layer 3** - Stream direction is indicated by the icon at the top of the column.

- **Duration** is the length of time the test ran.
- **Target Rate (bps)** is the requested bit rate from the SETUP tab.
- **Throughput (bps)** is the measured bit rate based on frames sent and the actual number of frames received.
- **Retries** (TCP Protocol only) is the number of retransmitted TCP segments.
- **Frames Sent** (UDP Protocol only) is the actual number of frames sent on the stream.
- **Frames Recvd** (UDP Protocol only) is the actual number of frames received on the interface.
- **Frames Lost** (UDP Protocol only) is the number of frames sent less the number of frames received.
- **Loss** (UDP Protocol only) is the percentage of frames that were lost.
- **Jitter** (UDP Protocol only) is the average frame delay variation.
- **Ping** shows the Ping response time from the iPerf server.

Note

If the Ping portion of the test fails, the entire iPerf test will fail.

- **Return Code** specifies the end-of-test status or an error condition if encountered.
- ⑪ **Wi-Fi Layer 2** - Shows average measurements:
- **Tx Rate (Mbps)** - The average transmission rate is shown in Mbps or Kbps.
 - **% Max Tx Rate (Mbps)** - The percentage of the maximum transmission rate is shown in Mbps or Kbps. When the average rate is less than 30% of the maximum rate, a warning icon ⚠ is displayed.
 - **Retries (% pkts)**- A warning icon ⚠ is displayed when the average retry rate exceeds 40% of total packets.

- **802.11 Utilization (% bw)** - 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.
 - **Non-802.11 Utilization (% bw)** - Non-802.11 utilization is reported in terms of the percentage of bandwidth usage on the connected channel.
- ⑫ **Return Codes** specify the end-of-test status or an error condition if encountered.
- ⑬ At the bottom-left corner of the screen, an icon indicates the test's status:
- 🌀 A progress spinner indicates the test is in progress.
 - ✓ A green check mark indicates the test passed.
 - ✗ A red x indicates the test failed.
- An error message indicates the reason for test failure.
- ⑭ Tap **CLEAR RESULTS** to clear all data on the screen.
- ⑮ Tap the **START** button to re-run the test for the current BSSID.

Performance Peer

This functions allows you to configure the OneTouch to act as a Performance Peer for a Wired or Wi-Fi Performance Test. See Chapter 5: "User Tests," beginning on [page 103](#), "Wired Performance Test" on [page 129](#) and "Wi-Fi Performance Test" on [page 144](#).

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 .
- 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/WebCam

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 126. 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**.

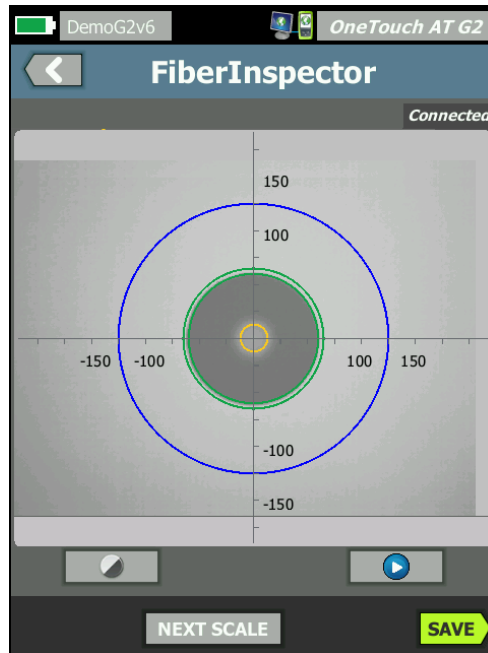



Figure 127. FiberInspector Image with Measurement Scales
(fiber with 50 μm core shown)



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 348](#)). 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.

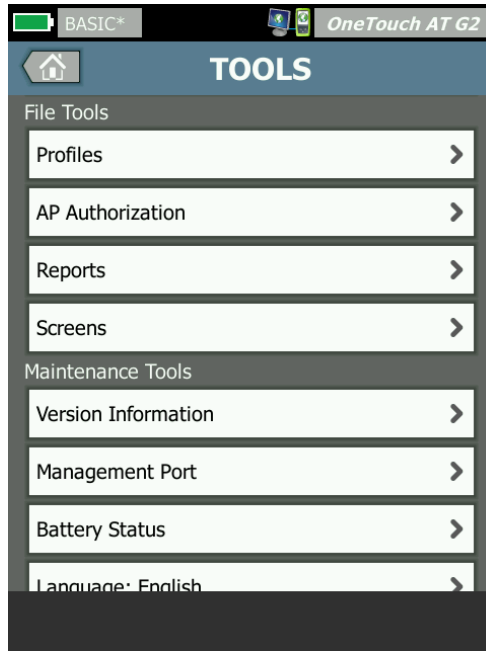


Figure 128. File Tools

Profiles

See Chapter 6: "Profiles," beginning on [page 161](#).

AP Authorization

See "Save an Authorization File" on [page 237](#).

Reports

The OneTouch analyzer can create a comprehensive report in PDF and/or XML format (for exporting to Excel). Specific report options are available when exporting to PDF: Tools Settings, AutoTest, Wired Analysis, Wi-Fi Analysis, VoIP Analysis, and Wi-Fi Network Validation. All available details are included when you save a report only in XML.

Note

*In addition to accessing the **Reports** options from the **TOOLS** screen, you can also tap the **OneTouch AT G2** short-cut button on the top right corner of your OneTouch screen to access available report options. See Figure 129.*

When you initially power on a OneTouch analyzer, and navigate to the Reports tool, only the Tools Settings report content option is shown.



Figure 129. Initial Available Report Options

You must run AutoTest to include AutoTest data in the saved report, and you must run Wi-Fi, Wired, or VoIP Analysis for those options to appear on the Save Report screen.

Obtaining Report Options

To see AutoTest, Wired Analysis, Wi-Fi Analysis, VoIP Analysis, or Wi-Fi Network Validation options included in your saved PDF report, follow these guidelines:


- To obtain AutoTest and Wired Analysis data in your report run AutoTest, select its check box on the Save Report screen, 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.
- To obtain Wi-Fi Network Validation data in your report, run Wi-Fi Network Validation, select its check box, and save.
- To obtain Path Analysis data in your report, run Path Analysis, tap the **Wired Analysis** button on the Save Report screen, select the Path Analysis 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.

Save a Report

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. The SAVE REPORT screens appears.



Figure 130. Save Report Screen—Possible Report Options

- 4 Tap the **File:** button to change the file name if desired, and then tap the **Done** button.
- 5 Tap the **Format:** button to change the report output if desired. Reports can be exported as a PDF, XML for export to an Excel file, or both.

Note

The report content options are only available when saving in PDF format. XML reports will contain all available details.

For **AutoTest**, **Wi-Fi Analysis**, and **Wired Analysis**, you can determine which summaries and details you want the report to include.



Figure 131. Report Content Options for AutoTest

- 6 Tap the back button  to go back to the Save Report screen.

- 7 Tap the **Wired Analysis** button to select wired analysis content for your report.

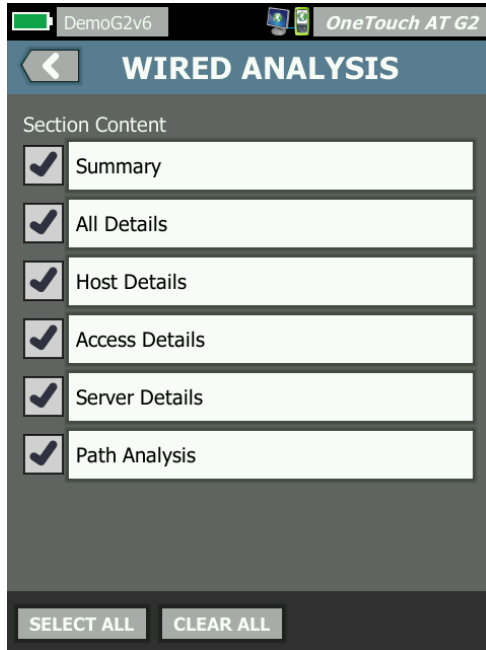



Figure 132. Report Content Options for Wired Analysis

To obtain Path Analysis data in your report, run Path Analysis using the Wired analysis screens. Then, tap the **Wired Analysis** button on the Save Report screen, select the **Path Analysis** check box, and save.

- 8 Tap the back button  to go back to the Save Report screen.

- 9 Tap the **Wi-Fi Analysis** button to select from available Wi-Fi Analysis report content options.

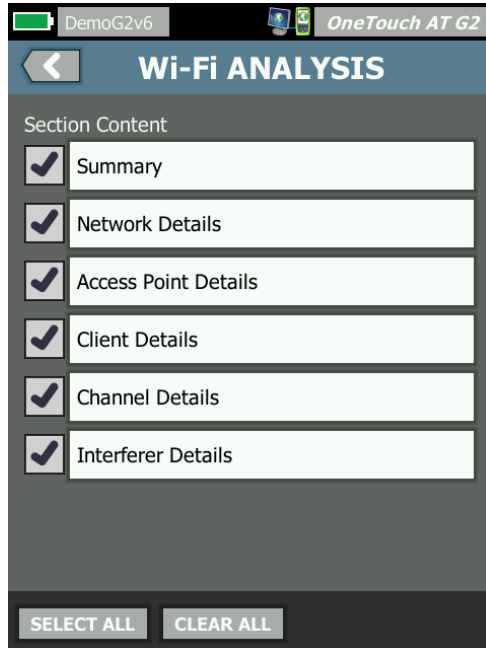



Figure 133. Report Content Options for Wi-Fi Analysis

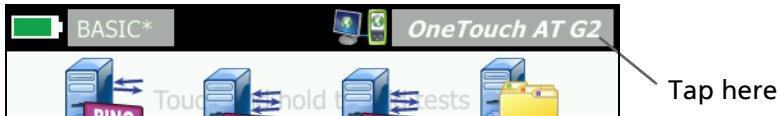
- 10 Tap the back button  to go back to the Save Report screen.
- 11 Use the check boxes next to Tools Settings, VoIP Analysis, and/or Wi-Fi Network Validation to include their data in your saved report. See Figure 130.
- 12 Tap the **SAVE** button. The report is saved in your selected format(s) to the analyzer's /internal/Reports directory. You can access the saved file as described in Chapter 11: "Managing Files," beginning on [page 341](#).
- 13 Tap **VIEW** to see the saved report on the OneTouch analyzer. See also: [page 344](#).

Screens

Save a Screen Image

You can take a screen shot of the OneTouch analyzer's display as follows:


- ① Tap the button that says OneTouch AT G2 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

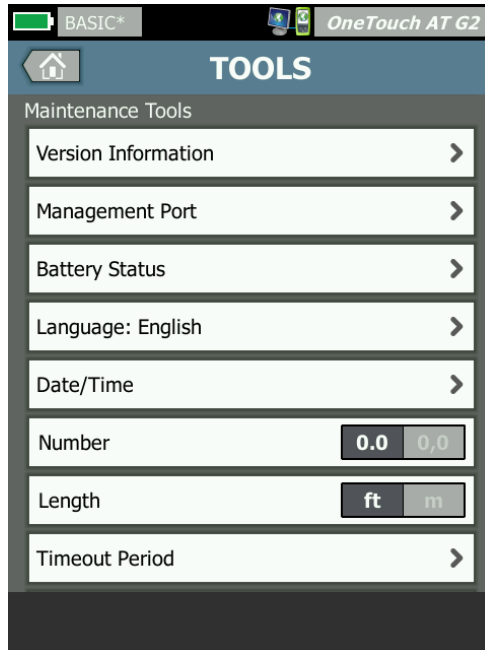



Figure 134. Maintenance Tools

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

Your OneTouch management port can be set to wired or Wi-Fi. The wired is the RJ-45 Ethernet port located on the left side of the OneTouch analyzer. The Wi-Fi management port is an optional Wi-Fi adapter that can be connected to the OneTouch AT's USB port on the right side of the device. The adapter can be ordered separately from NETSCOUT.

The wired management port is the default management port. It links automatically when connected to a network. It is not necessary to run AutoTest to make either of the management ports link. However, if you go into the Management Port configuration screen and make any changes to the management port settings, you will need to select the CONNECT button for any changes to take effect.

The Wi-Fi Management port is disabled by default and needs to be configured on the Management Port configuration screen prior to use.

To configure the Wi-Fi management port:

- 1 Insert the Wi-Fi management port adapter into the OneTouch AT's USB port.
- 2 On the HOME screen, tap **TOOLS** .

- 3 Scroll down to the Maintenance Tools section and tap **Management Port**. The management port screen is displayed.





Figure 135. Management Port Screen Linked Wired

- 4 On the **Active Port** button, tap **Wi-Fi**.
- 5 Tap the **Wi-Fi** button.
- 6 Tap the **Address** button, then tap **DHCP** or **Static**.
Selecting **Static** will show additional selections: **IP**, **Subnet Mask**, **Gateway**, **DNS1**, and **DNS2**. You must provide a static IP address and a Subnet Mask.
- 7 Tap the **SSID** button.
- 8 Tap an **SSID** from the list of available SSIDs.
- 9 Tap the **Security** button. It will take you to the Security screen.
- 10 Tap the **Type** button if you want to change the current setting.

If you change the security type, additional selections will become available. These additional selections will vary depend-

ing on the selected authentication type.

- 11 Tap each new selection that became available as a result of changing the authentication type and provide the requested information.
- 12 Tap the back button  to return to the initial Management Port screen.
- 13 Tap the **Connect** button  for your new settings to take effect.

Management Port Selections

User/Password - This option is **Off** by default. When it is **On**, the **User** and **Password** buttons will be shown.

User - Assign a user name to the management port.

Password - Assign a password to the management port.


Active Port - Choose **Wired** or **Wi-Fi**. **Wired** is the default. When choosing **Wired**, a network cable must be connected to the RJ-45 port. When choosing **Wi-Fi**, the optional Wi-Fi management port adapter must be connected to the OneTouch USB port.

Wired - Select **DHCP** or **Static IP** addressing.


Wi-Fi - allows you to choose **DHCP** or **Static IP** addressing, select an **SSID**, and choose an authentication option. Connect the optional Wi-Fi management port adapter to the OneTouch AT's USB port.

Configure Login Credentials for Remote Access

To configure user name and password for remote access via management port:

- 1 On the **HOME** screen, tap **TOOLS** .
- 2 Scroll down to **Maintenance Tools** and tap the **Management Port** button.
- 3 On the **User/Password** button tap **On**. This action will display the **User** and **Password** buttons on the screen.

- 4 Tap the **User** button and enter a user name.
- 5 Tap the **Password** button and enter a password.
- 6 Choose an Active Port: Wired or Wi-Fi. Ensure that if you choose the Wired Port, a cable is connected to the Wired management port, and if you choose Wi-Fi that the Wi-Fi management port adapter is connected to the USB port.

If you select Wi-Fi, you may have to configure it. Follow the directions in the procedure above.
- 7 Tap the **Connect** button  for your new settings to take effect.

Address Control (DHCP or Static)

The Address control can be set to DHCP or Static. When set to DHCP, the 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 251](#).

The OneTouch analyzer's management ports 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

Battery Status

This screen shows the battery's status.

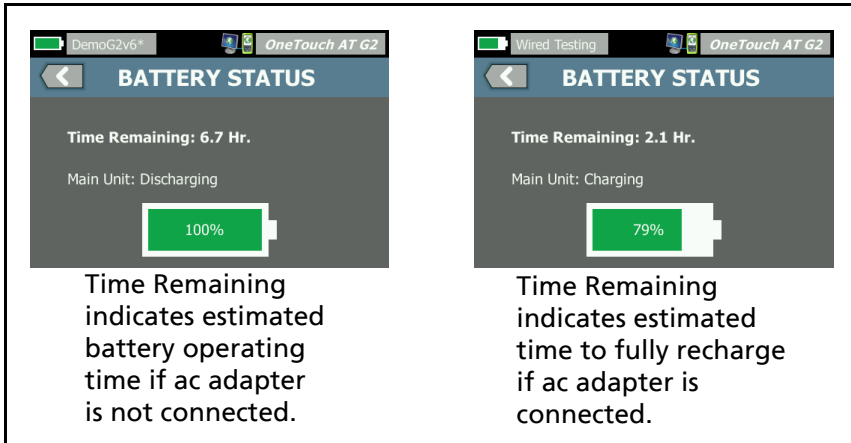


Figure 136. Battery Status Screen

Language

See "Set the Language" on [page 7](#).

Date/Time

See "Date/Time" on [page 29](#).

Number

See "Number Format" on [page 30](#).

Length


See "Units for Length Measurements" on [page 30](#).

Timeout Period

See “Timeout Periods (Power-Down and Backlight)” on [page 30](#).

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

See “Power Line Frequency” on [page 30](#).

Display

- 1 On the HOME screen, tap **TOOLS** .
- 2 Scroll down to the Maintenance Tools section, and tap **Display**.
- 3 Move the yellow bar to select the desired brightness.
- 4 Tap the **DONE** button.

Note


Increasing the display brightness draws more power, thereby decreasing run-time when operating the OneTouch analyzer on battery power.

Update Software

To prevent problems caused by losing power during a software update, supply power to the OneTouch analyzer with the AC adapter.

Updating Software Using a USB Drive or SD card


To update software, download the new software image file from <http://enterprise.netscout.com>. You can install the new software image file from a USB flash drive or an SD card.

- 1 On the HOME screen, tap **TOOLS** .
- 2 Scroll down to the Maintenance Tools section and tap **Software Update**.
- 3 Navigate to the directory where you saved the new software image (.img) file and select the file.
- 4 Select the **OK** button.
- 5 Select **YES** to install the new file.

The new file will be installed and the analyzer will restart. The process will take several minutes.

Updating Software via Link-Live Cloud Service

Starting with OneTouch version 6.5.1, you can download updates from Link-Live if your OneTouch is claimed. (See also “Link-Live Cloud Service” on [page 359](#).) To download major releases, you must have Gold Support.

- 1 On the HOME screen, tap **TOOLS** .
- 2 Scroll down to the Maintenance Tools section and tap **Software Update**.
- 3 On the Update Software screen, touch the **CHECK UPDATE** button. A pop-up dialog box informs you if an updated firmware version is available.
- 4 Touch **YES** to download the firmware.


- 5 Select a storage location for the update file by answering **YES** or **NO** when the options are shown. After you touch **YES**, the **.img** file will download to the selected location.
- 6 Navigate to the directory where you saved the new software image file, and select the file.
- 7 Select the **OK** button to install the new firmware.
- 8 Select **OK** again to confirm.

The new file will be installed and the analyzer will restart. The process will take several minutes.

Options

If you did not purchase your OneTouch analyzer with all options enabled, you can purchase and activate options at a later time.


Enter an option's product key to activate the new option.

- 1 On the HOME screen, tap **TOOLS** .
- 2 Scroll down to the Maintenance Tools section.
- 3 Tap **Options**.
- 4 Enter the product key. You may be asked to restart the analyzer by cycling power to the analyzer.

To purchase options, contact NETSCOUT. See [page 6](#) for contact information.

Export Logs

If you have reason to contact our Technical Assistance Center, you may be asked to send log files from the analyzer to the customer service representative.

- 1 On the HOME screen, tap **TOOLS** .
- 2 Scroll down to the Maintenance Tools section.
- 3 Tap **Export Logs**.
- 4 Ensure that an SD card is inserted in the analyzer.

- 5 Tap **OK** to export the log files to the SD card.

Factory Defaults (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 10: 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 NETSCOUT (see [page 6](#)).

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 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 137.

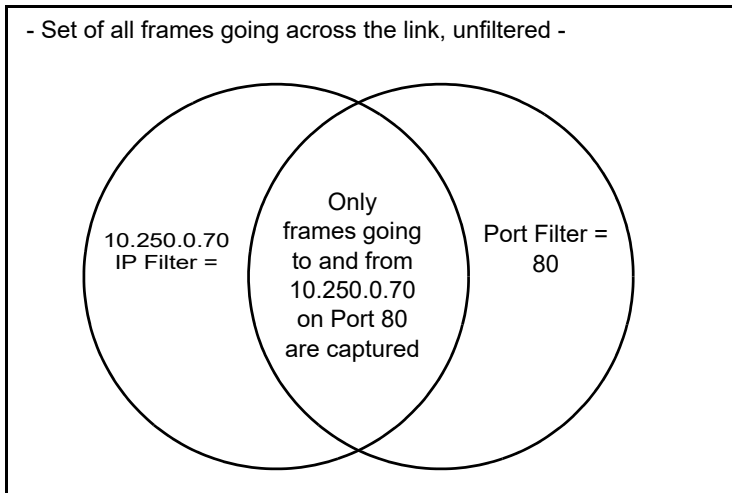


Figure 137. Capture Filters - Logical AND Operation

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.

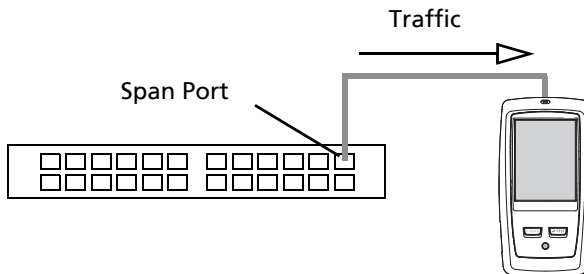


Figure 138. Single-Ended Packet Capture

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.

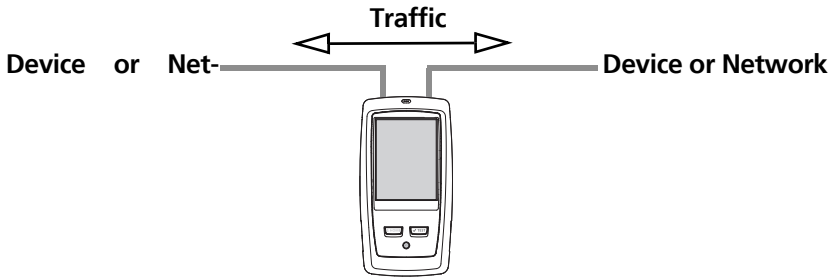



Figure 139. Inline Packet Capture

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 319](#).
- Traffic is passed between the two ports as soon as they are linked. 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.

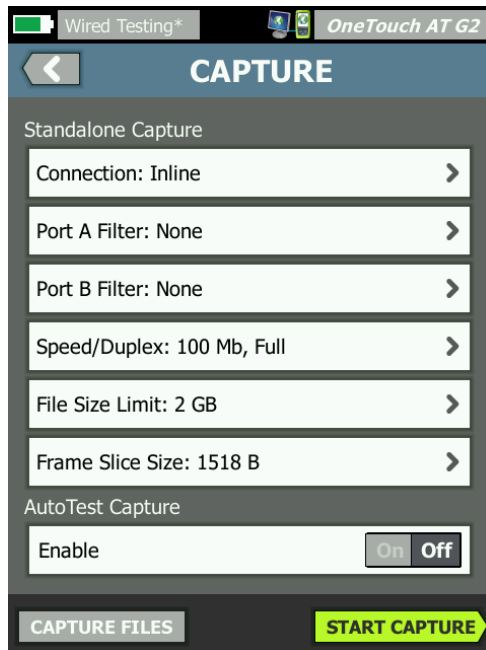


Figure 140. The Wired CAPTURE Screen

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.

Speed/Duplex

When using packet capture, set the speed and duplex in the capture configuration to match the link where you are inserting the OneTouch AT analyzer. If Auto is selected, the OneTouch will link on both ports at the fastest common speed and duplex detected.

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 334](#)

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  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



Figure 141. Wi-Fi Test Settings Screen

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


To review the other Wi-Fi connection settings, see Chapter 3, “Establish a Wi-Fi Connection” on [page 48](#).

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.



Figure 142. 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

The analyzer can capture on 20 MHz, 40 MHz, or 80 MHz wide channels. 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. Access points supporting 802.11ac allow capture from 20, 40, or 80 MHz channels (OneTouch AT G2 only). Adjacent 20 MHz subchannels are grouped into pairs to make 40 MHz channels, and adjacent 40 MHz subchannels are grouped into pairs to make 80 MHz channels.

When capturing traffic for an access point that is configured to use a 40 MHz 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 Acknowledgment (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 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 325](#).

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 334](#)

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  appears in the lower-right corner of the screen.
- 3 Tap the **TOOLS** button.
- 4 Tap the **Capture** button.

- For dual-band APs or APs that support multiple SSIDs, select the BSSID and channel of interest.

Cisco4400 Cisco:0017df-a10fdf	Ch: 1		-45 dBm
Cisco4400_WPA2o... Cisco:0017df-a10fd2	Ch: 64		-53 dBm

The CAPTURE screen is displayed and the filter configuration is indicated on the **Wi-Fi Filter** button.



Figure 143. Wi-Fi CAPTURE Screen

- 6 Tap the **Wi-Fi Filter** button. The CAPTURE SETTINGS screen is displayed.

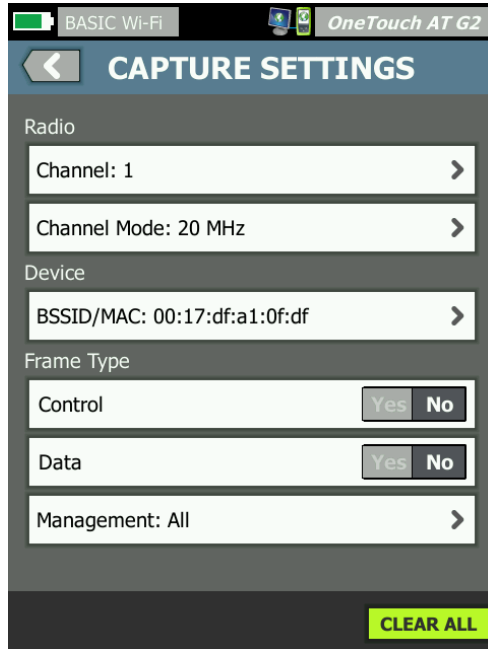


Figure 144. CAPTURE SETTINGS Screen


From this screen, you can further modify your capture settings.

For more information see “To Manually Configure a Filter” on [page 327](#).

To start the capture see “Start Packet Capture” on [page 334](#).

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  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 327](#).

To start the capture see "Start Packet Capture" on [page 334](#).

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  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 327](#).

To start the capture see "Start Packet Capture" on [page 334](#).

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.

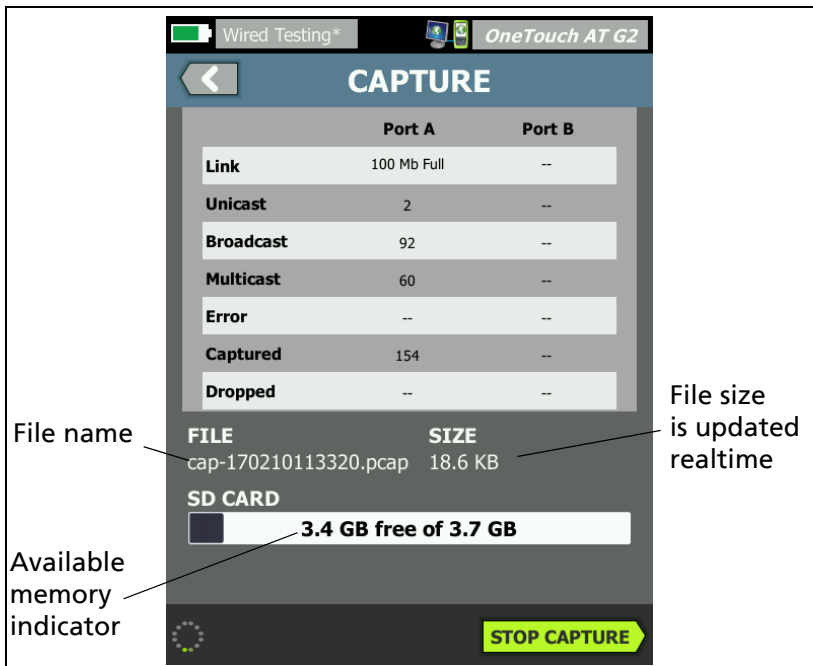


Figure 145. Wired Capture Results

As a Wi-Fi packet capture progresses, management, control, data, and total frame counts are shown.

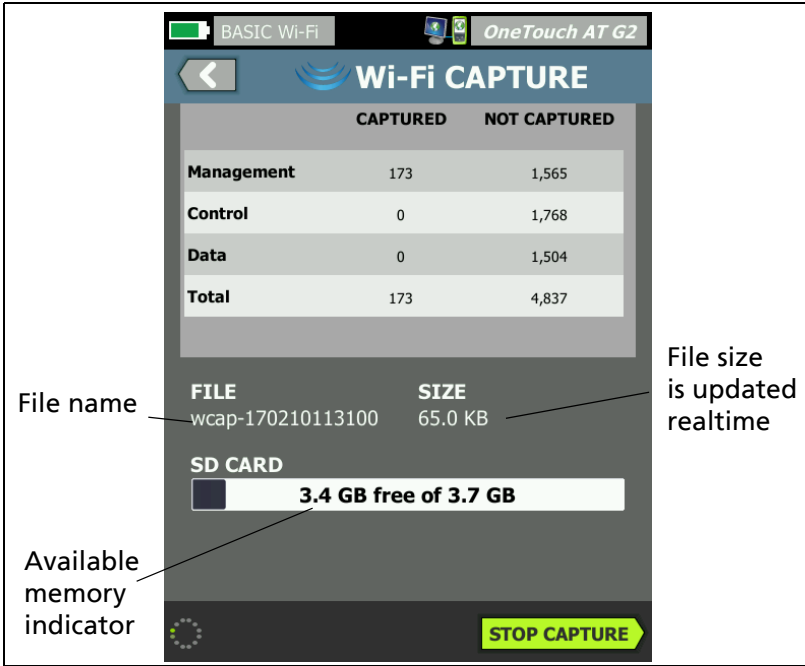


Figure 146. Wi-Fi Capture Results

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 re-appears. Failure to wait for the **START CAPTURE** button to re-appear may result in loss or corruption of SD card data.*

AutoTest Capture

The OneTouch AT 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  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 .

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 341](#).

Analyzing Capture Files

You can use ClearSight Analyzer software or other protocol analysis software to analyze the captured packets on a PC.

Chapter 11: 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](#).

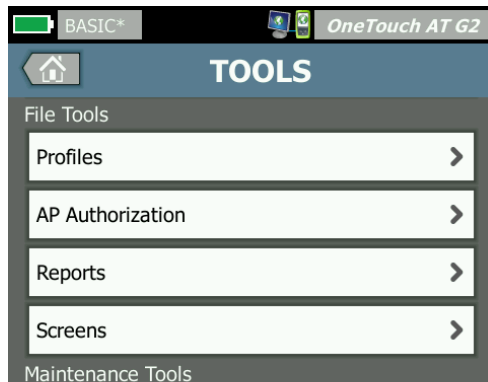
Packet captures can be managed using the Capture tool. See [page 338](#).

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.

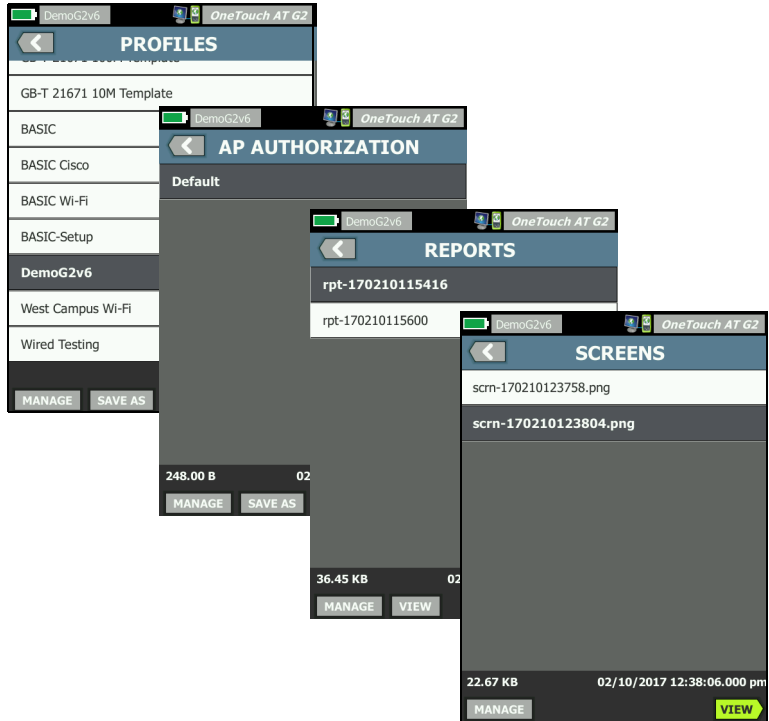


Figure 147. The Four File Manager Screens

The following section describes buttons that are available on one or more of the file manager screens.

SAVE

The **SAVE** button saves the current profile, AP authorization list, or report.

When you tap the **SAVE** button, the SAVE AS screen is displayed.



Figure 148. 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 20](#).

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.

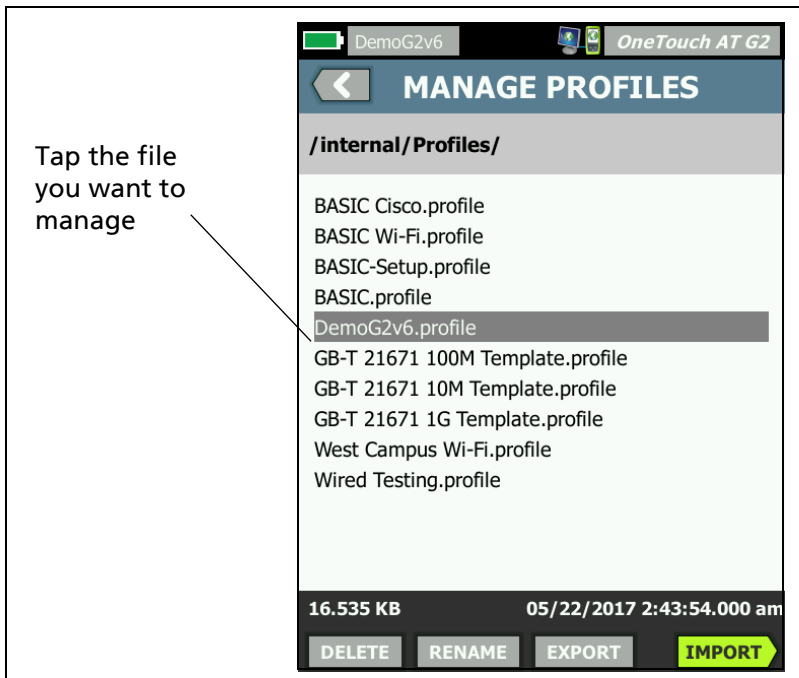


Figure 149. Manage Profiles Screen

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 .pdf or .xml file to internal memory, an SD card, or a USB flash drive. Tap the **EXPORT** button to show the navigable file tree.

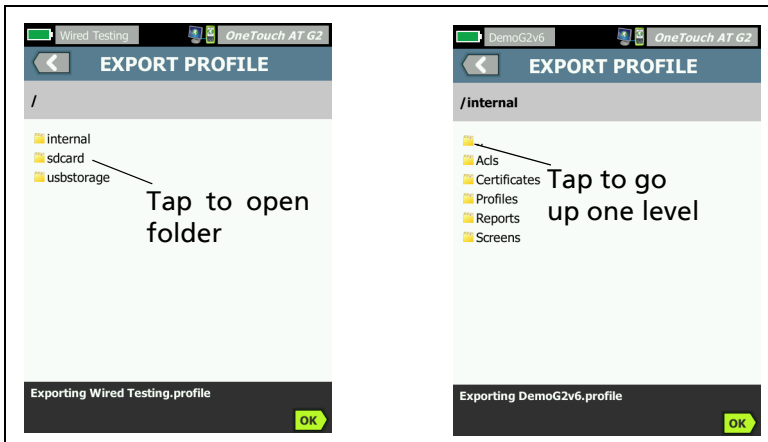


Figure 150. File Manager - Export File Tree

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, reports, 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 or .xml 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 control of the OneTouch analyzer's user interface is possible through a VNC client connection and in the "[Link-Live Cloud Service](#)".

Note

For more information on accessing and remote controlling your OneTouch in Link-Live, see Chapter 13: "Link-Live Cloud Service," beginning on [page 359](#).

To remotely access the file system, connect via Link-Live, FTP, a web browser, or a mapped network drive (WebDAV).

You can set up remote access security by configuring the OneTouch analyzer's management port.

User Interface Remote Control

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 308](#).
- 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 310](#).

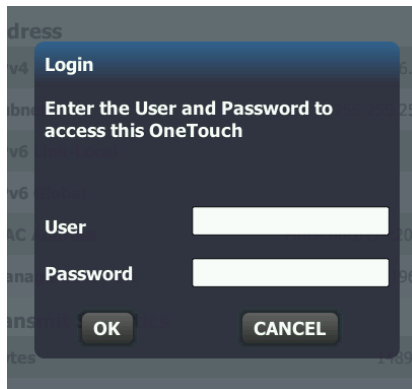


Figure 151. Browser Remote Access Login Credentials

- 5 Navigate the user interface with your pointing device (mouse, touch screen, etc.) to select items.

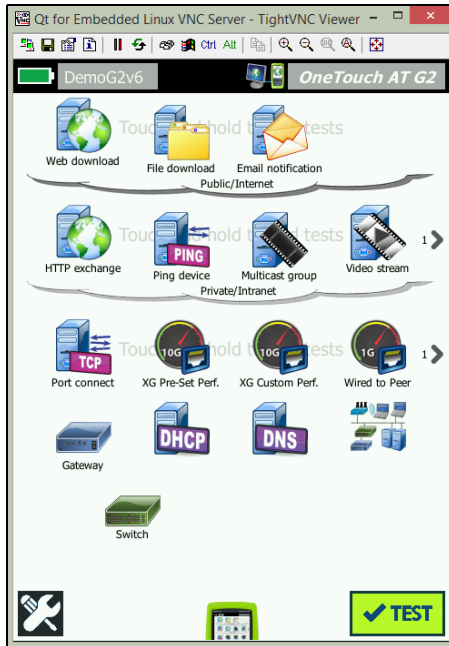


Figure 152. Remote Access OneTouch Home Screen

Remote Control Using the Link-Live Cloud Service

See "Remote Access from the Cloud" on [page 365](#).

Remote File Access

You can remotely access files on the OneTouch analyzer using an FTP, Link-Live, a web browser, or a network drive mapped with WebDAV.

Remote File Access Using a Web Browser

To access the OneTouch analyzer's user file system using a web browser:

- 1 Obtain the IP address of the management port as described on [page 297](#).
- 2 Open a web browser.
- 3 Enter the OneTouch analyzer's Management Port IP address in the web browser's field.
- 4 If required, enter the OneTouch analyzer's remote access user name and **password**. See also: "Configure Login Credentials for Remote Access" on [page 300](#).

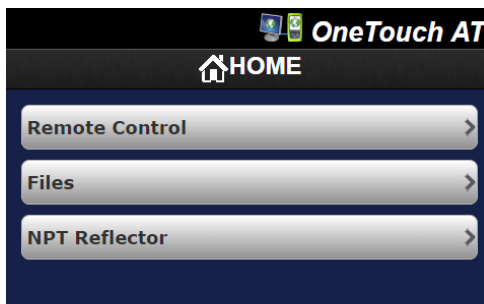


Figure 153. OneTouch Web Server Home

- 5 Select the **Files** button.
- 6 Navigate the user interface with your pointing device (mouse, touch screen, etc.) to select items.

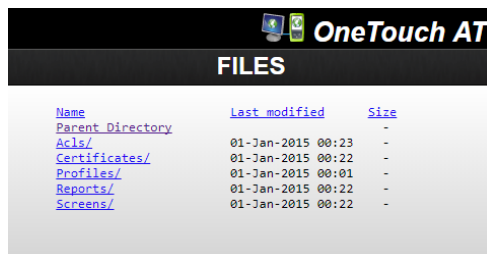


Figure 154. OneTouch Remote File Access

- 7 To download an item, right click its name, and select "Save [target/link/image] as...".

Note

You cannot delete, rename, move, or upload files using a Web Browser.

Remote File Access Using an FTP Client

To connect to the OneTouch analyzer's user file system with an FTP Client:

- 1 Obtain the IP address of the management port as described on [page 308](#).
- 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 computer.


- 1 Obtain the IP address of the management port as described on [page 308](#).
- 2 Select the Windows **Start** button, or open **File Explorer**.
- 3 Right-click **Computer** or **This PC**.
- 4 Select **Map network drive...**

- 5 In the Map Network Drive dialog, select an available drive letter.
- 6 Enter the path to your 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: "Configure Login Credentials for Remote Access" on [page 310](#).

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 155. Remote Access icon located in Shortcut Bar

- 2 Select the **Disconnect** button.

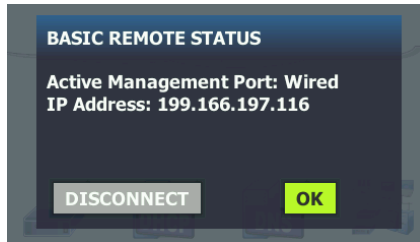


Figure 156. Management Port Status Dialog - Remote Control Disconnect

- 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 14](#). 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 13](#). The OneTouch analyzer supports FAT and FAT32 file systems on external media.

Chapter 12: Maintenance

Maintenance

Warning

To prevent possible fire, electric shock, personal injury, or damage to the analyzer:

- The battery is the only user serviceable component. Do not open the case except to replace the battery.
- Use only replacement parts that are approved by NETSCOUT.
- Use only service centers that are approved by NETSCOUT.

Clean the Analyzer

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

To clean the case, use a soft cloth that is damp with water or a mild detergent solution.

Caution

To prevent damage to the touchscreen do not use abrasive materials.

To prevent damage to the case, do not use solvents or abrasive materials.

Extend the Life of the Battery

To extend the amount of time the battery will provide satisfactory operation before it needs to be replaced:

- Recharge the battery frequently. Do not let the battery discharge completely.
- Do not keep the battery in hot areas.
- Before you put a battery into storage, charge it to approximately 50% of full charge.

Store the Analyzer

- Before you store an analyzer or an extra battery for a long period, charge the battery to approximately 50% of full charge. The discharge rate of the battery is 5% to 10% each month. Check the battery every 4 months and charge it if necessary.
- Keep a battery attached to the analyzer during storage. If you remove the battery for more than approximately 24 hours, the analyzer will not keep the correct time and date.
- See “Environmental and Regulatory Specifications” on [page 367](#) 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 157.

Use only NETSCOUT battery model 1T-BATTERY.

Note

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

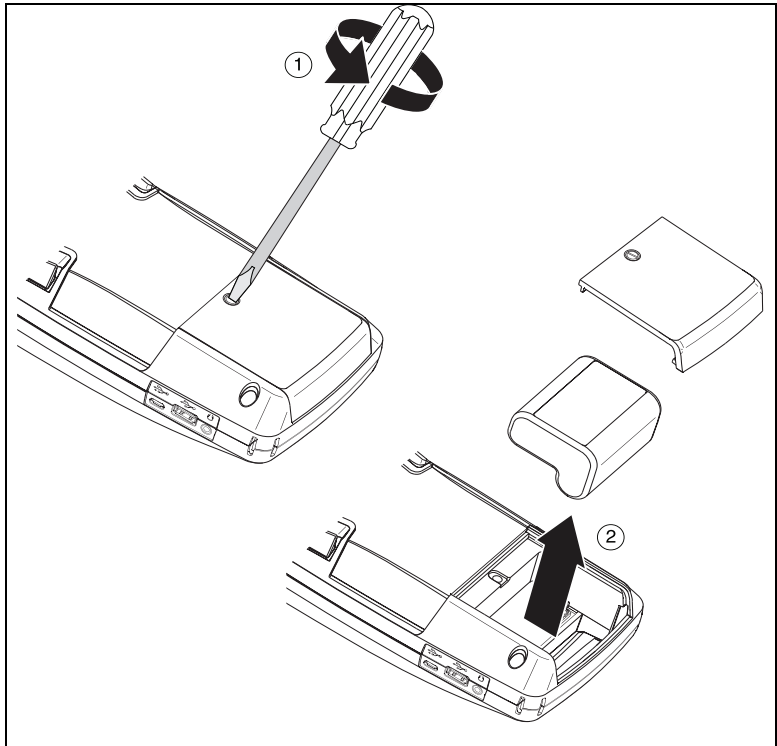


Figure 157. Remove and Install the Battery

GVO003.EPS

Chapter 13: Link-Live Cloud Service

Overview

The OneTouch AT G2 allows you to send test results to your Link-Live.com Cloud Service account, where those results can be viewed, organized, and managed from a web-enabled device.

In addition to viewing and analyzing results, you may remotely access and update your OneTouch AT G2 analyzer through the cloud service, as well as configure your OneTouch to automatically upload reports of your test results to Link-Live for storage and retrieval.

Link-Live Cloud Service Support Page

For detailed information on using the Link-Live Cloud Service to manage your OneTouch AT test results and reports, go to <https://app.link-live.com/support>, or from Link-Live.com, click

 Support >  Questions.

Infrastructure and User Tests in the Cloud

Test result trends from the following tests can be managed in the cloud:

Infrastructure Tests

- Nearest Switch
- Gateway
- DHCP
- DNS

User Tests

- Ping (ICMP)
- Connect (TCP)

- Web (HTTP)
- File (FTP)
- 1G Wired Performance (RFC 2544)
- Wi-Fi Performance
- Video (RTSP)
- Email (SMTP)

Setting Up and Accessing the Cloud Service

The following steps will help you set up and get started using your Link-Live Cloud Service.

- 1 Create or sign in to your [Link-Live.com](https://link-live.com) account.
- 2 **Claim** your unit.
- 3 Enable **Upload AutoTest** to send results to Link-Live.
- 4 Create a unique name for your OneTouch analyzer.
- 5 Go to Link-Live.com to manage your test results.

To begin setup from the OneTouch HOME screen, tap **TOOLS**  and scroll down to **Link-Live Cloud Tools**.

Creating a Link-Live.com Account

To create a Link-Live.com account:

- 1 Go to <https://app.link-live.com/signup>.
- 2 Enter the appropriate information on the web page, and click **CREATE ACCOUNT**.

Claiming Your Unit

The process to claim your analyzer includes both the unit and the Link-Live Cloud website. You must have a user account to claim your unit.

Note

A claimed unit is associated with the currently active Organization. See the Link-Live.com Support page for more information about Organizations.

To claim a unit:

- 1 In [Link-Live.com](#), navigate to the **Units** page from the left sidebar.
- 2 Click the **Claim Unit** button at the lower right of the page.
- 3 Select your device (OneTouch), and follow the prompts on the Link-Live website.


Once your OneTouch analyzer is successfully claimed, you should see a successful claim message on Link-Live.com, and the claim status on the unit should update to **Claimed**.

Setting up Periodic AutoTest

When the analyzer is in Periodic AutoTest mode, the OneTouch analyzer runs AutoTests at specified intervals and sends the results to Link-Live so that you can view the results over time. Periodic AutoTest is helpful when baselining network performance or troubleshooting intermittent problems.

Periodic AutoTesting can be set up only after a unit has been claimed. Your unit must be connected to a network for this process to work. Your results can be sent through either of the network test ports or the management port.

To enable Periodic AutoTest:

- 1 Select **TOOLS**  from the HOME screen.
- 2 Under **Link-Live Cloud Tools**, select **Periodic AutoTest**.

Note

A shortcut to the Periodic AutoTest screen is to touch and hold the Test button on a unit's HOME screen.

- 3 Configure the following:
Duration - The length of time during which test results will be

sent to the Link-Live Cloud. The duration can be set to Unlimited Duration, 2, 5, 10, and 30 minutes, or 1 hour, 2 hours, 3 hours, 4 hours, 5 hours, 6 hrs, 8 hrs, and 12 hrs, or 1 day, 2 days, 3 days, 4 days, 5 days, or 1 week, or 2 weeks.

Interval - This is the amount of time between sent test results to the Link-Live Cloud over a selected time duration.

Comment - This entry will appear beneath the Periodic Auto-Test results in Link-Live Cloud Service. Use this feature to annotate your Periodic AutoTest session.

Backlight Timeout - This feature controls how long the One-Touch screen's backlight stays illuminated while Periodic Auto-Testing is ongoing.

This option is disabled by default. You can set the backlight to turn off automatically after 5, 10, or 15 minutes, extending the life of the screen. When the backlight turns off, you can tap the screen to turn it back on.

- 4 Tap the **Launch** button.

Periodic AutoTest setup is successful when a translucent PERIODIC AUTOTEST STATUS screen is displayed on the unit's

HOME screen and shows an IP address.

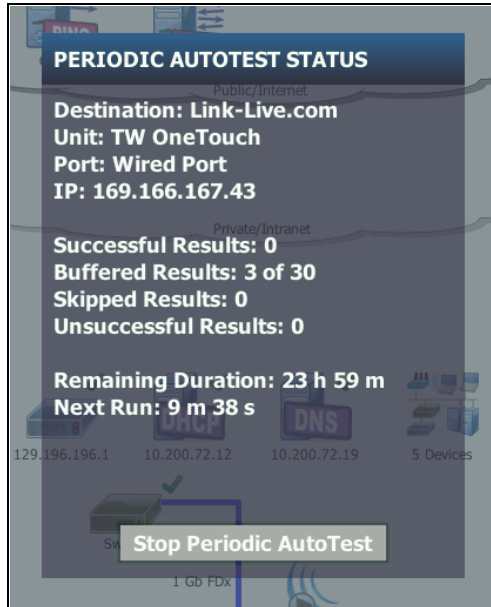


Figure 158. Periodic AutoTest Status Screen

Periodic AutoTest Status Screen

The Periodic AutoTest Status screen (Figure 158) shows the following information:

Destination: shows the web location of where the AutoTest results are sent.

Unit: shows the unit name.

Port: the port that the Periodic AutoTest process will use to send results to the cloud. It can be the network test ports, the RJ-45 management port, or the optional Wi-Fi management port.

IP: the IP address of the Periodic AutoTest port currently in use.

Successful Results: the number of successful runs to Link-Live.com after the completion of an AutoTest, regardless if the AutoTest passed or failed.

Skipped Results: If an AutoTest run did not complete during the time assigned for the interval, that run will be skipped. For example, if the assigned interval was 1 minute long and the AutoTest is taking 3 minutes to complete (for various reasons: test retries, port issues, etc), the assigned interval time will be too short and the run will be skipped.

Unsuccessful Results: The number of unsuccessful runs to Link-Live.com after the completion of an AutoTest, regardless if the AutoTest passed or failed.

Remaining Duration: The amount of time left in a specified Periodic AutoTest duration. Refers to the Duration time assigned on the OneTouch AT in **Tools > Link-Live Cloud Tools > Periodic AutoTest**.

Next Run: The amount of time until the next AutoTest run begins. Refers to the interval time assigned on the unit in **Tools > Periodic AutoTest**.


Naming your OneTouch AT

By default, the analyzer's name is its serial number. We recommend that you rename your OneTouch AT to a familiar or descriptive name.

Note

When you claim a OneTouch AT G2 unit to Link-Live Cloud Service, the name entered on Link-Live is reassigned to the OneTouch.

To rename your analyzer on the unit:

- 1 On the analyzer HOME screen, tap **TOOLS** .
- 2 In the **Link-Live Cloud Tools** section, tap **Unit Name**.
- 3 Enter a descriptive name for your OneTouch AT.
- 4 Tap **DONE** when finished.

Remote Access from the Cloud

You can connect remotely to a claimed OneTouch AT analyzer and choose to control the analyzer or view its user files on Link-Live.com.

The claimed unit must be part of your organization or belong to an organization of which you are a member.


Preparing Your Unit for Remote Access


Before your analyzer can be accessed from the Link-Live Cloud, the **Cloud Remote** option needs to be enabled on the unit.

Note

If the unit is not enabled for remote cloud access, it can still be accessed from a VNC client via the management port address.

To enable remote cloud access:

- 1 On the analyzer's HOME screen, tap **TOOLS** .
- 2 In the **Cloud Tools** section, touch the **Cloud Remote** button to open the CLOUD REMOTE screen.
- 3 Enable remote access to the OneTouch by switching the toggle to **On**.

A **Cloud Remote** icon  will be shown on the unit at the top of the screen.

Chapter 14: Specifications

Environmental and Regulatory Specifications

Operating temperature¹	32°F to 122°F (0°C to 50°C)
Storage temperature²	-40°F to 160°F (-40°C to 71°C)
Operating relative humidity (% RH without condensation)	5% to 45% at 32°F to 122°F (0°C to 50°C) 5% to 75% at 32°F to 104°F (0°C to 40°C) 5% to 95% at 32°F to 86°F (0°C to 30°C)
Shock and vibration	Meets the requirements of MIL-PRF-28800F for Class 3 Equipment
Safety	CAN/CSA-C22.2 No. 61010-1-04 IEC 61010-1:CAT none, pollution degree 2
Operating altitude	13,123 ft (4,000 m) 10,500 ft (3,200 m) with AC adapter
Storage altitude	39,370 ft (12,000 m)
Pollution degree	2
EMC	EN 61326-1:portable
<p>1 The battery will not charge if its temperature is outside the range of 32°F to 104°F (0°C to 40°C).</p> <p>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.</p>	

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 connector¹	Reverse SMA
1 External antenna port is receive-only (no transmit).	

Wi-Fi Adapter

Applicant's name	NETSCOUT
Equipment name	Wi-Fi testing device
Model number	WA7-43460AC
Manufacturing Year/ Month	2015/06
Manufacturer	Universal Global Scientific Industrial Co. (USI)
Country of origin	Taiwan

OneTouch AT and OneTouch AT G2
User Manual

<p>Data rate</p>	<p>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 802.11ac (80 MHz): MCS0NSS1-MCS9NSS3 (20, 40, and 80 MHz bandwidth), up to 1300 Mbps</p>
<p>Operating frequency</p>	<p>2.412 ~ 2.484 GHz (Industrial Scientific Medical Band) 5.170 ~ 5.825 GHz</p>
<p>Security</p>	<p>64/128-Bit WEP Key, WPA, WPA2, 802.1X</p>
<p>Transmit output power¹ (tolerance: ±2.0 dBm)</p>	<p>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 802.11ac VHT20: 13 dBm ± 2 dBm @ MCS8NSS3 802.11ac VHT40: 13 dBm ± 2 dBm @ MCS9NSS3 802.11ac VHT80: 11 dBm ± 2 dBm @ MCS9NSS3</p>

Receive sensitivity (tolerance: ± 2 dBm)	802.11a: $-81 \text{ dBm} \pm 2 \text{ dBm} @ 54 \text{ Mbps}$ 802.11b: $-92 \text{ dBm} \pm 2 \text{ dBm} @ 11 \text{ Mbps}$ 802.11g: $-82 \text{ dBm} \pm 2 \text{ dBm} @ 54 \text{ Mbps}$ 802.11gn HT20: $-79 \text{ dBm} \pm 2 \text{ dBm} @ \text{MCS7}$ 802.11gn HT40: $-76 \text{ dBm} \pm 2 \text{ dBm} @ \text{MCS7}$ 802.11an HT20: $-78 \text{ dBm} \pm 2 \text{ dBm} @ \text{MCS7}$ 802.11an HT40: $-74 \text{ dBm} \pm 2 \text{ dBm} @ \text{MCS7}$ 802.11ac VHT20: $-64 \text{ dBm} \pm 2 \text{ dBm} @ \text{MCS8NSS3}$ 802.11ac VHT40: $-63 \text{ dBm} \pm 2 \text{ dBm} @ \text{MCS9NSS3}$ 802.11ac VHT80: $-60 \text{ dBm} \pm 2 \text{ dBm} @ \text{MCS9NSS3}$
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

	Conformite Europeene. Conforms to the requirements of the European Union and the European Free Trade Association (EFTA).
	Listed by the Canadian Standards Association.
	The Product complies with Australian standards.
	Conforms to relevant South Korean EMC Standards

Electromagnetic Compatibility. Applies to use in Korea only. Class A Equipment (Industrial Broadcasting & Communications Equipment)	This product meets requirements for industrial (Class A) electromagnetic wave equipment and the seller or user should take notice of it. This equipment is intended for use in business environments and is not to be used in homes.
--	--

Memory

Internal memory	The OneTouch 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

FCC ID: WA7-43460AC

IC ID: 6627C-43460AC

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 and FCC ID: WA7-43460AC.

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.

Regulatory Statements

<p>Brazil Regulatory Statement</p>	<p>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.</p>
<p>Korea Electromagnetic Compatibility. Applies to use in Korea only. Class A Equipment (Industrial Broadcasting & Communications Equipment)</p>	<p>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.</p>
<p>Mexico Cofotel Notice</p>	<p>La operación de este equipo está sujeta a las siguientes dos condiciones: (1) es posible que este equipo o dispositivo no cause interferencia perjudicial y (2) este equipo o dispositivo debe aceptar cualquier interferencia, incluyendo la que pueda causar su operación no deseada.</p>
<p>Taiwan Regulatory Compliance Warning for Access Points according to rule of LP0002</p>	<p>低功率電波輻射性電機管理辦法 經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。</p> <p>低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。</p> <p>前項合法通信，指依電信法規定作業之無線電通信。</p> <p>低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。</p>

— Notes —

— Notes —