

Application Note: Managing BYOD and the Consumerization of IT

OneTouch AT Network Assistant Application Handbook



TABLE OF CONTENTS

- » Introduction
- » How do I understand the inventory of Wi-Fi devices?
- » How do I identify undesired networks?
- » What if a rogue AP is using the enterprise SSID?
- » Can I locate an offending AP, hotspot or ad-hoc device?
- » What if a rogue AP is not broadcasting its SSID?
- » Has someone set up an ad hoc network?
- » Are there any unexpected clients on my corporate SSID?
- » Why is the performance bad in this area?
- » How do I verify that my Wi-Fi QoS is working?
- » How can I tell more about the Wi-Fi device?
- » How do I verify proper access for my various SSIDs?
- » Is my Wi-Fi offloading working?
- » How can I authenticate through my guest SSID?
- » I'm here but my problem isn't. What do I do?
- » Is this a wireless or wired problem?
- » How does my Wi-Fi transaction performance compare to my wired?
- » How do I identify BYO hubs, switches and routers?
- » Can I get enough power to my Access Points?
- » What if I need to capture traffic?
- » Conclusion

Introduction

The consumerization of IT is fast becoming a reality in many if not all corporate IT departments. The proliferation of tablets and other smart devices has increased dramatically in the past several years and use of these 'consumer class' products on enterprise networks is nearly ubiquitous. A recent study showed 90% of organizations polled allow some level of personally owned technology to be used on site—a phenomenon known as BYOD (Bring Your Own Device). In addition to the wave of phones and tablets as clients, readily available low cost residential gateways, routers, APs and switches can creep into the enterprise. Confident in their newfound home networking skills, employees are more emboldened than ever, creating network entropy.

The influx of mobile clients and network equipment have many in IT looking for the best way to detect, inventory, audit, locate and manage the flood of new devices. In a recent survey, 62 percent report that their company lacks the necessary tools to support employee personal devices, regardless of whether policies are in place or not. Fears and concerns abound. Managing the impact of personal devices, protecting corporate data and intellectual property, and auditing to ensure compliance are a thorn in the side of most IT departments.

The Fluke Networks OneTouch™ AT Network Assistant has a variety of features that provide the visibility and control to harness the BYOD explosion and reduce the risks and operational costs associated with delivering a secure, high performance, pervasive, reliable wired and wireless infrastructure. The OneTouch has a unique combination of wired and wireless analysis features in a rugged package that is as mobile as the devices it manages. This application note explores the practical application of the Fluke Networks OneTouch AT Network Assistant for a variety of common BYOD issues facing IT such as:

- How to inventory the state of your current Wi-Fi network
- How to investigate user complaints regarding performance and connectivity
- How to identify rogue clients, APs and other network devices
- How to audit network permissions
- How to measure Wi-Fi performance
- How to test coverage of cellular handoffs



How do I understand the inventory of Wi-Fi devices?

Most Wi-Fi in the enterprise is experiencing explosive usage as networks previously supporting only corporate laptops handle a barrage of diverse phones and tablets. In addition to the growth of the total number of devices, the appetite for bandwidth can disrupt the performance of mission-critical enterprise applications. The key to dealing with the BYOD phenomenon is to understand just how pervasive it is. You must inventory the devices, see what networks and access points they are connecting to, and find out how healthy the air is.

The OneTouch automatically discovers and categorizes Wi-Fi under four tabs: Network, AP, Client and Channel. Sorting by properties allows multiple views into the wireless network. For example, sort by signal strength to troubleshoot Wi-Fi coverage issues. Sort by utilization to identify AP, client or channel utilization problems. Sort by authorization status to find potential security violations. Sort by MAC manufacturer to discover Wi-Fi devices by type and to understand how they are connected relative to SSID, AP and channel.

The Client tab displays all wireless devices that the OneTouch is seeing on all channels. Here it is possible to audit compliance to formal policies used by IT in supporting BYOD. Android devices are typically represented by Samsung, HTC and Motorola manufacturer codes, and Blackberry is represented by RIM. Figure 1 is an example. We can quickly identify outliers such as the Apple device on channel 161, a 5 GHz channel, and another Apple device probing for its known SSIDs but not connected to the network.

Tapping on any of the devices expands the view to show detailed information about the network, SSID, channel and security in use by the device, and begins detailed trending of key device indicators. See Figure 2. Filter buttons provide deeper analysis of each client's related networks, access points and channels used.

When you approach your Wi-Fi analysis from the most relevant domain (SSID, AP, client or channel), sorting and filtering is a versatile way to understand the inventory. Tapping the OneTouch AT button in the upper right corner lets you capture a screen (take a screen shot) or create a detailed PDF report to document your BYOD inventory.

The OneTouch is Wi-Fi vendor agnostic and can be used at your desk, walking a hallway, or left behind for remote operation.



Figure 1

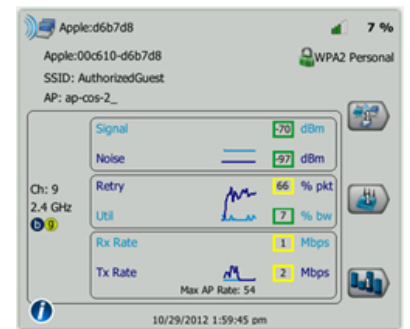


Figure 2

How do I identify undesired networks?

Low cost access points and mobile hot spots can pose a performance and security risk on the corporate network. A mobile phone hotspot can be used to allow connection to the internet without using the corporate LAN/WAN. While the portable hotspot is backhauled through the cellular network, it still shares the air with the enterprise Wi-Fi network. This can lead to channel congestion or co-channel interference.

Even more problematic than the portable 3G hotspot is the employee that brings in a residential AP or gateway to create a personal Wi-Fi network for their tablets and phones by plugging the gateway into the corporate network. This results in not only air congestion, but unauthorized Wi-Fi access to the corporate LAN.

The OneTouch performs Wi-Fi Analysis by constantly scanning the air, channel by channel, characterizing SSIDs, APs, clients and channel usage. The analysis is presented in four tabs, with the ability to sort the analysis many different ways. For example: to detect potential rogue Wi-Fi networks, select the Networks tab and sort by Fewest Access Points. See Figure 3. This provides a fast way to identify one-off networks that have a single SSID supported by only a single AP. Additional indications of an undesired network are open networks, as indicated by the red open lock icon.

Selecting any SSID expands the network details. See Figure 4. Normal enterprise Wi-Fi networks provide coverage and capacity using multiple APs that are carefully positioned and assigned to non-overlapping channels. The number of APs, channels, and client supporting the SSID are shown on the filter buttons on the right of the display, and tapping a button provides a means to show only those devices.

The SSID "cody-dlink" has only one AP, which is connected to one host and is using one channel. See Figure 5. This is not representative of a normal corporate network, and may indicate a rogue AP. Sorting is a powerful tool for identifying outlier networks, access points, clients and channels.

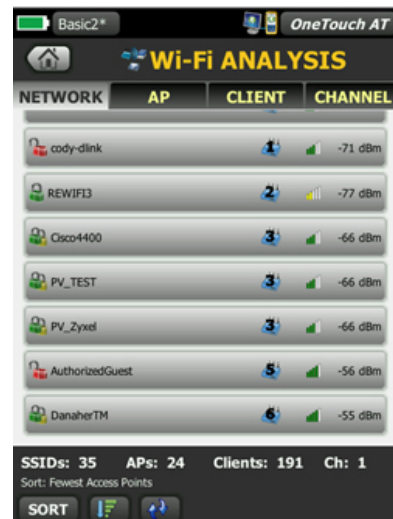


Figure 3

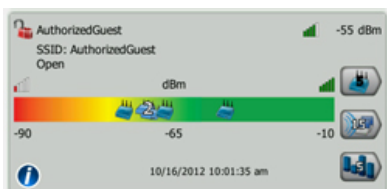


Figure 4

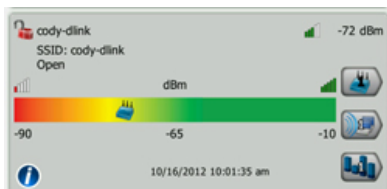


Figure 5

What if a rogue AP is using the enterprise SSID?

What if the worker sets their device SSID to match an enterprise SSID in an attempt to mask their private network? Starting on the Network tab and expanding a sanctioned corporate SSID such as Authorized Guest, we can immediately see it is supported by 4 APs. See Figure 6. Selecting the AP button unleashes the powerful filtered view. Tabs allow you to select an analysis starting point based on SSIDs, AP, client or channels, and the three filter buttons allow you to easily narrow down your investigation.

When filtering, the title bar changes from Wi-Fi Analysis to the sourcing filter criterion, in this case Authorized Guest. See Figure 7. We immediately see that the SSID is supported by three Cisco APs but also a Linksys device, which implies it may not be part of the corporate network.

You can use the OneTouch to proactively identify rogue and other devices that are new to the network. You can mark known APs in your premise, as well as nearby APs. Known and expected corporate APs can be marked as Authorized. See Figure 8. Off premise but known APs can be marked as Neighbors. The marking of APs is remembered by the OneTouch. Once expected APs are tagged, sorting by Authorization Status quickly identifies Unknown Access points such as the Linksys in the Authorized Guest screen shown in Figure 8.

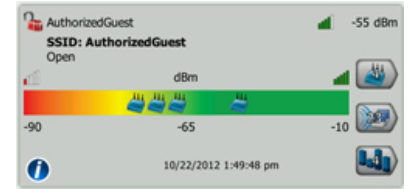


Figure 6

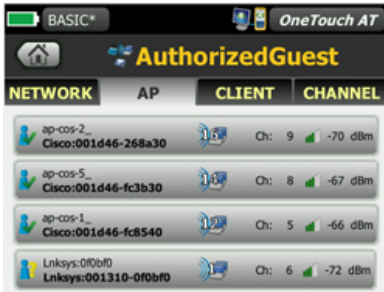


Figure 7



Figure 8

Can I locate an offending AP, hotspot or ad-hoc device?

Once a rogue AP or mobile hotspot is identified, the OneTouch provides a couple of ways to locate the device. Using the external directional antenna (see Figure 9) and Locate feature (see Figure 10) the physical location of any wireless device, AP or client, can be quickly found.

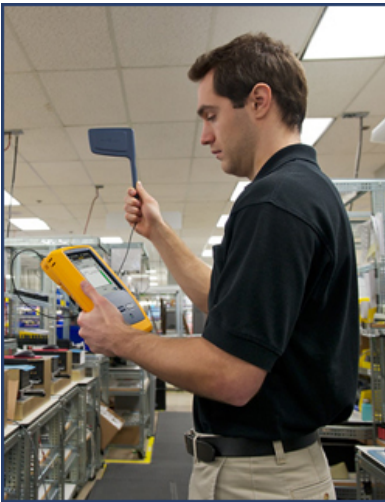


Figure 9

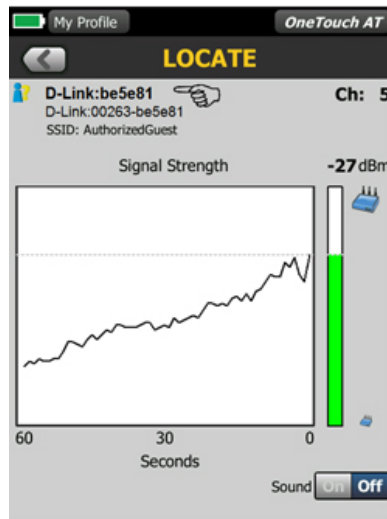


Figure 10



316 Devices

In the case of a rogue AP plugged into the wired network, you may be able to locate the switch slot and port to which it is connected using the OneTouch Wired Analysis. The device and user can be cut off by unplugging them from the network at the patch panel or by disabling the switch port.

To find a Wi-Fi Analysis device in Wired Analysis, sort wired analysis by MAC address and look for the wireless MAC address. See Figure 11. Note that in some cases adjacent

MAC addresses are used by multi-interface devices. In this case a D-Link device at an adjacent MAC address is attached to slot 2/port 44 of COS_DEV_SW1 using the IP address 10.250.1.176 on VLAN 500.

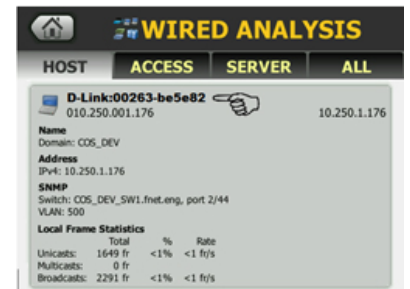


Figure 11

What if a rogue AP is not broadcasting its SSID?

What if a worker configures their AP to NOT broadcast its SSID in an attempt to go undetected on the corporate network? By identifying non-broadcasted networks, OneTouch helps you manage network usage and mitigate security issues.

OneTouch actively listens for non-broadcasted networks and reports the SSID as [Hidden] in the list of discovered networks. See Figure 12. Select the AP filter buttons to identify the AP using that non-broadcasted network. Using tools you can mark an unauthorized AP for proactive identification or locate the offending AP.

If you know the SSID of the hidden network, OneTouch sends an active probe request that includes specific SSIDs to an AP to resolve non-broadcasted SSIDs. OneTouch probes for all the SSIDs configured in all of its profiles on the instrument and passively learns about non-broadcasted SSIDs being used on the network from 802.11 packets. These resolved non-broadcasted SSIDs will be reported in brackets such as [BlackHole]. See Figure 13.

Has someone set up an ad hoc network?

What if a small group of workers have configured their laptops to operate in ad hoc mode for gaming? Although Ad hoc networks can have their place in an enterprise environment, they are more often against IT policy and can pose a security risk if configured as an unsecured, open network and corporate data is compromised. Ad hoc networks can also impact network performance if using same channel as corporate AP's.

Sorting by Network Type brings discovered ad hoc networks to the top of the list. See Figure 14. You can immediately see the ad hoc network name (Montana) being used and whether the network is secured or not. Expand the network to get more details about the network. Use the client filter to identify and locate the devices that comprise the network.

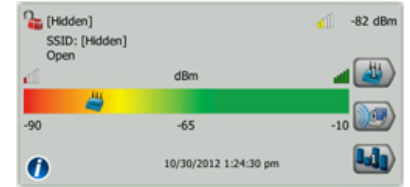


Figure 12

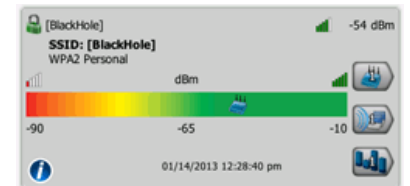


Figure 13



Figure 14

Are there any unexpected clients on my corporate SSID?

The only way that IT staff can maintain control over mobile device proliferation is by separating mobile computing devices into three distinct device classes: trusted standard devices provided by the company, tolerated devices and non-supported devices. It is good practice to make sure that the full access, corporate SSIDs only have expected APs and Clients. From the Network tab we selected our corporate SSID. See Figure 15. The AP icons on the AP strength indicator bar show that the SSID has good coverage by 4 APs on 4 different channels and is running enterprise security. To audit the clients on the selected SSID, simply tap the Client filter button to see the clients.

The title bar indicates the filtered SSID. See Figure 16. To make the list of the 37 clients more digestible we sort the list by Manufacturer MAC. This groups common devices. The list reveals that there are 36 corporate laptops with Intel MAC addresses attached to the SSID, but somehow an Apple device has managed to associate to the corporate network. This device may be allowed or not, per company policy. If not allowed the device can be located using the wireless directional antenna or possibly by finding the device MAC in Wired Analysis as described previously.

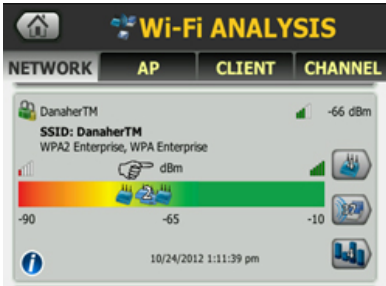


Figure 15

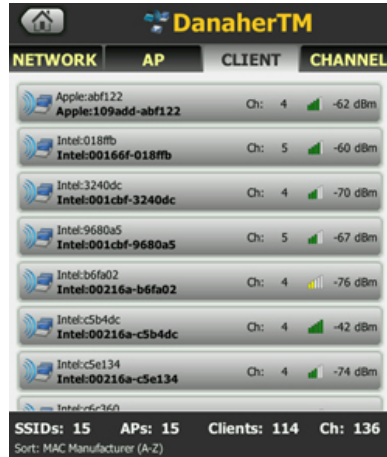


Figure 16

Why is the performance bad in this area?

One of the pitfalls of supporting BYOD is that it can be difficult to maintain mission critical corporate Wi-Fi access in the presence of personal devices. Congested airspace and high bandwidth use models such as streaming video can hamper mission critical communications. What happens when a manager complains of performance issues on VoIP calls from a meeting room?

In this case, the portability of the OneTouch coupled with Wi-Fi analysis is unmatched. Head to the problem area and use the Wi-Fi Analysis Client tab and identify the complaining client. Alternately, you could use the network tab and client filter to narrow the search. In Figure 17, we see that the signal level is strong. Also note that a steady signal level is indicative of a client that is not moving. The noise level is low, indicating that the air is generally healthy and void of non-802.11 interferers. However the retry rate is high, as indicated by the yellow color grading. Also the Rx and Tx rates are quite variable.

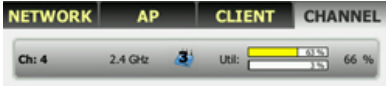


Figure 18

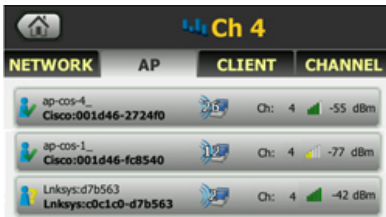


Figure 19

Selecting the channel filter button takes us to channel 4, (see Figure 18) where we see high 802.11 utilization indicated by the yellow bar. To determine the source of the utilization we filter on APs.

Filtering on channel 4 APs (see Figure 19), we see three APs. Two are our enterprise APs, which are heavily loaded with 38 clients. But we also see a strong, nearby LinkSys AP with 2 clients. It is unexpectedly sharing our channel. Use the location techniques previously presented to locate the AP.

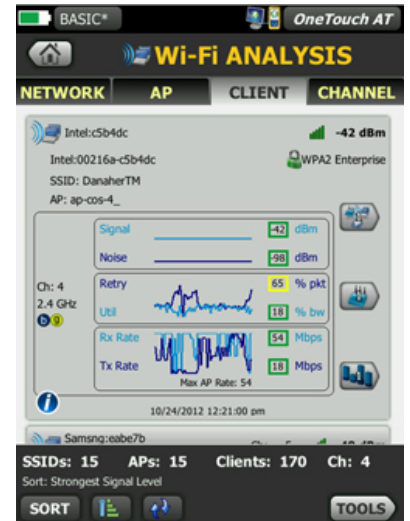


Figure 17

How do I verify that my Wi-Fi QoS is working?

With the influx of personal user devices, it is critical to verify Wi-Fi performance & prioritization of production traffic over best effort user data traffic. Quality of service (QoS) enables Wi-Fi access points and switches to prioritize traffic. Without QoS, all applications running on different devices have equal opportunity to transmit data frames. Industry standards such as 802.11e and WME (Wireless Multimedia Extensions) prioritize traffic from different devices and applications to extend a high quality end-user experience to mission critical traffic such as voice under a wide variety of environmental and traffic conditions. QoS traffic shaping can be rendered using a variety of mechanisms such as SSIDs, ports, or DSCP.

The OneTouch Veri-Fi™ feature allows quick, deterministic verification of wired/Wi-Fi performance by streaming data between the OneTouch wired and wireless interfaces. See Figure 20. Veri-Fi can be used in a variety of ways:



Figure 20

- To measure Wi-Fi upstream and downstream performance
- To generate large amounts of background traffic to verify that critical QoS is not impacted when the AP is loaded.
- To verify that QoS is not impacted by the best effort traffic.

In this example we will test that VoWi-Fi traffic using the DSCP Expedited Forwarding (EF) value of 46 is provisioned correctly. See Figure 21. Additionally, we will verify that the QoS works over both IPv4 and IPv6. We select a VoIP RTP representative Frame Size of 128 bytes and specify a symmetrical data rate of 1Mbps upstream (Wi-Fi →Wired) and downstream (Wired →Wi-Fi) to approximate 10 simultaneous calls. The test results (displayed as frame loss rate) are below the pass/fail limit of 1%, so the test passes. See Figure 22. Background traffic can be generated using personal devices or a second OneTouch.

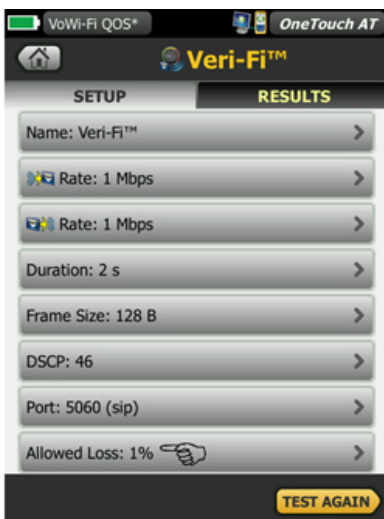


Figure 21

	IPv4	IPv4	IPv6	IPv6
Rate (bps)	1.0 M	1.0 M	1.0 M	1.0 M
Frames Sent	244	244	244	244
Frames Recvd	243	244	244	244
Frames Lost	1	0	0	0
Loss	0.41%	0%	0%	0%
Actual (bps)	999 k	1 M	1 M	1 M
Latency	2 ms	1 ms	1 ms	1 ms
Jitter	2 ms	<1 ms	<1 ms	<1 ms
Out Of Seq	0	0	0	0
Ping	1 ms	1 ms	1 ms	1 ms

Figure 22

How can I tell more about the Wi-Fi device?

Wi-Fi analysis gives us an unprecedented view of wireless networks, access points, clients and channels. In the case of clients (Figure 23) we can see the following information:

- MAC Address
- SSID (Network)
- AP
- Security
- Radio Type (a/b/g/n)
- Channel and band
- When last seen
- One minute trends of key indicators

We can also easily filter to the associated Network, AP and Channel. However since everything above the source and destination MAC is encrypted, including layer 3 IP addresses, it is often desirable to learn more about the device through wired analysis.

In many cases the OneTouch Wired Analysis can discover the IP address, VLAN and even the name assigned to the device through discovery and interrogation of the wireless LAN controller. A wireless device can be found by sorting the Wired Analysis by MAC address and matching it to the Wi-Fi MAC address. In Figure 24 we see that the Apple device with the MAC address of 40a6d9-b46809 is seen on the wired network with an IP address of 10.250.0.135 on VLAN 500. The VLAN information is useful to verify that the device is operating on the appropriate VLAN relative to its authorization level or user group. You can use the OneTouch wired analysis to scan the wired device for open ports to learn more about the device; in this case the iphone-sync TCP port 62078 is open.

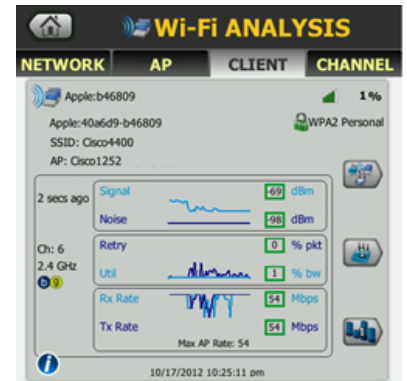


Figure 23

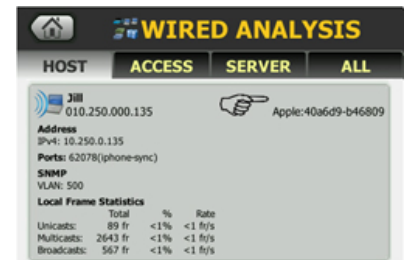


Figure 24

How do I verify proper access for my various SSIDs?

Enterprises typically implement access network zones to limit the connectivity of personally owned mobile devices using multiple SSIDs that in turn control network access.

Permission	Access	SSID
Full Access	Internet & all corporate resources	AcmeCorp
Partial Access	Internet & some corporate resource	AcmeContractor
Internet Only	Internet only	AcmeGuest

BYOD requires policies and provisioning to control which corporate resources clients are allowed to access. SSIDs are often segmented using unique IP addressing and wired VLANs to control access.

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

In Figure 25 we see a profile called Contractor Access that tests connectivity to both allowed and disallowed services. The tiers are renamed to group the test as allowed and disallowed.

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

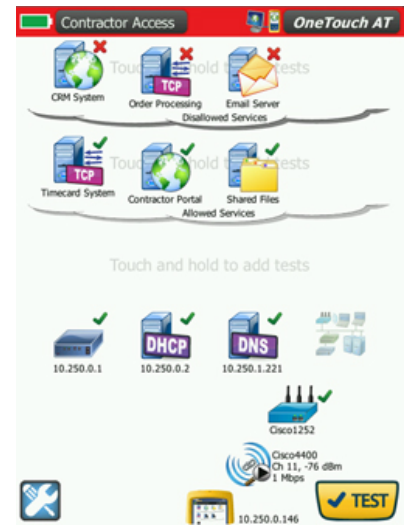


Figure 25

Is my Wi-Fi offloading working?

The ability to roam seamlessly within an enterprise is fundamental to today's BYOD users. Offloading to Wi-Fi from cellular offers many benefits including:

- Lower data charges
- Faster connections
- Lower battery drain
- Improved end user experience

But how do you make sure that your Wi-Fi coverage is sufficient to prevent thrashing (constant channel hopping) between radios?

Once connected to an SSID, the OneTouch tracks coverage from one AP zone to another. The OneTouch records the details of each roam as you walk your facility. You can use the roaming results navigation controls to view the details of each associated AP. See Figure 26. For each AP, the minimum and maximum values for signal, noise, retries and utilization provide insight into the operating range of AP zone.

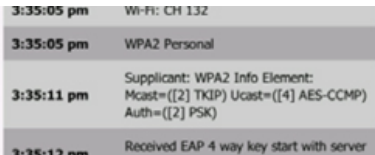


Figure 27

Tap the LOG tab to view the time stamped details of each connection, authentication and association. See Figure 27.

Using the Ping (ICMP) tool during the roaming, we can also find dead spots in coverage that could result in a 3G on-loading. By targeting an internal ping responder, not reachable through cellular, we ensure that we lose data when not connected to Wi-Fi. In Continuous ping mode with a one second time limit; the number of lost ping packets equals the number of seconds without Wi-Fi. See Figure 28. In this case Wi-Fi was lost for 6 seconds of the 228 seconds roaming. This test can also be conducted using the Connect (TCP) test to perform a TCP port open to the selected target to test for application port reachability. More comprehensive coverage testing can be achieved using AirMagnet Survey and AirMapper™.

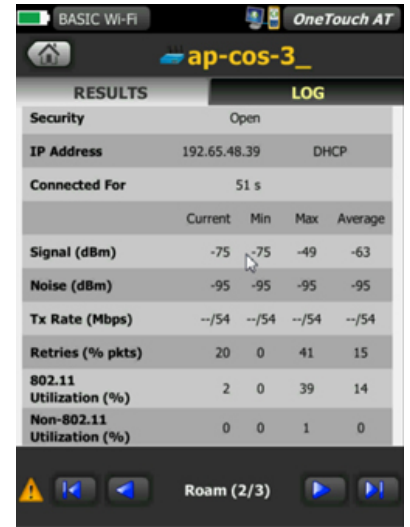


Figure 26

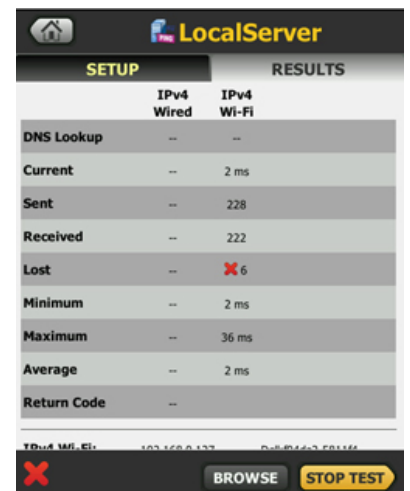


Figure 28

How can I authenticate through my guest SSID?

When connecting to guest and hospitality Wi-Fi networks, it is typical to have to authenticate or accept terms into a captive portal. The captive portal forces an HTTP client on a network to see a special web page before using the network.

The OneTouch integrated web browser can operate through the management, wired or Wi-Fi test ports. In Figure 29 the OneTouch analyzer uses its Wi-Fi port to access a web page and the browser is redirected to a web page which may require authentication and/or payment, or simply display an acceptable use policy and require the user to agree. Once authenticated, the OneTouch Wi-Fi test port MAC address is typically cached, allowing 24 hours of access. If a captive portal is being used on the wired test interface as in a wired hotel room, the same technique can be used to authenticate the wired interface.

In addition to navigating through captive portals, the OneTouch integrated web browser can be used to provision network elements such as switches and Wireless LAN controllers. See Figure 30.

The OneTouch analyzer also includes an integrated SSH/Telnet for command line provisioning and diagnostics. See Figure 31.



Figure 30



Figure 31



Figure 29

I'm here but my problem isn't. What do I do?

Wi-Fi is a very challenging media. Besides dynamic bandwidth demands, clients come and go, as well as sources of interference. For example BYOD OS upgrades, updates to popular apps, cloud backup or even a viral video can strain a network. What happens when you walk across the campus to diagnose a client problem only to find the problem doesn't exist at the moment?

Connecting the OneTouch analyzer to the network via its management port allows you to leave the unit behind and operate it remotely. This allows you to resume other work and periodically check the Wi-Fi from your desk, or when the client calls again.

Simply point your web browser or VNC client at the management port IP address and go. You can operate the OneTouch from your desktop, laptop, tablet or phone on the go. See Figure 32. The OneTouch analyzer's user interface, with large touchable icons, makes it easy to operate even from a phone. If you see something strange you can tap the OneTouch AT button at the top of the screen to save a report or capture a screen to document the intermittent problem.



Figure 32



Figure 33

The OneTouch analyzer is so versatile you can even plug a common webcam into the USB port to do remote surveillance. For example, you can watch the number of participants in a meeting room, observe a screen or display, or monitor the LEDs on a piece of network equipment. This allows you not only monitor the network but also the physical space. See Figure 33.

Is this a wireless or wired problem?

Wi-Fi presents a different access to the network using RF for layer 1 and 802.11 for layer 2. But once you get past the access points, you are dependent on the same underlying wired infrastructure. Besides the Wi-Fi analysis techniques presented so far, the OneTouch analyzer has a plethora of Wired Analysis features that also play a role in BYOD management. The OneTouch analyzer's Wired Analysis sorts operate similarly to those in Wi-Fi Analysis. Sorting by Problems quickly bubbles any discovered wired problems to the top of the list. See Figure 34. Tapping on any device reveals more details.



Figure 34

For example in Figure 35, the wireless LAN controller (WLC) rebooted 12 minutes ago and might be responsible for the current trouble ticket(s). Using SNMP, the OneTouch analyzer also reports the location of the device and owner. Other sorts include IPv4 address, IPv6 address, MAC address, manufacturer name, top broadcaster, domain, and more.

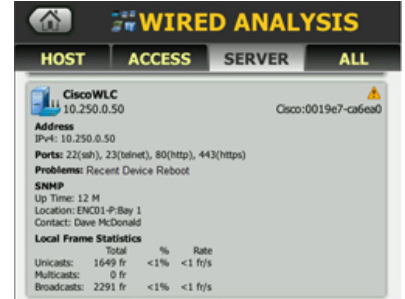


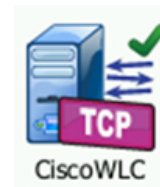
Figure 35

Sorting by VLAN (Figure 36) allows verification that BYOD devices are correctly sequestered to their designated VLAN associated with their SSID.



Figure 36

Any discovered device can be further probed using the built in port scanner. Additionally, Wired Analysis is useful to identify key Wi-Fi devices. You can build AutoTest profiles to create standardized tests that quickly determine the availability of critical network equipment and diagnose its condition.





How does my Wi-Fi transaction performance compare to my wired?

Sometimes it is difficult to know if the bottleneck is the Wi-Fi or the rest of the network. The OneTouch analyzer simultaneously tests your wired Ethernet and Wi-Fi networks and easily compares performance with side-by-side test results. This comparison extends to IPv6 when enabled in the OneTouch analyzer's wired setup.

In Figure 37 we use the FTP user test to measure the end user response time (EURT) of a one megabyte file download. The use of FTP depends upon the underlying TCP performance, which is also shown in the test results. The FTP tool allows for either file download (get) or upload (put).

The *Total Time* (EURT) is the the sum of the individual times that make up the transaction:

- *DNS Lookup* is the amount of time used to resolve the URL to an IP address.
- *TCP Connect* is the amount of time used to open the port on the server.
- *Data Start* is the time it took to receive the FTP file data frame from the server.
- *Data Transfer* is the amount of time it took to transfer the file data.

The precisely timed, side by side comparison of wired and wireless performance coupled with the breakdown of the transaction components is invaluable in determining whether your Wi-Fi is the bottleneck or not.

If the Total Time exceeds the Time Limit you selected the test will fail. Therefore, you can create an AutoTest profile to test the end user experience. Note that depending on the location of the FTP server, the bottleneck may be WAN capacity, in which case the Wired and Wi-Fi data transfer times would be similar. Other useful and comparative user tests include web, multicast, and RTSP for video subscription.

SETUP	RESULTS			
	IPv4 Wired	IPv4 Wi-Fi	IPv6 Wired	IPv6 Wi-Fi
DNS Lookup	<1 ms	1 ms	1 ms	1 ms
TCP Connect	1 ms	9 ms	342 ms	41 ms
Data Start	12 ms	18 ms	16 ms	28 ms
Data Transfer	206 ms	387 ms	178 ms	594 ms
Total Time	219 ms	415 ms	537 ms	664 ms
Data Bytes	1 M	1 M	1 M	1 M
Rate (bps)	40.1 M	21.3 M	46.4 M	13.9 M
Ping	6 ms	8 ms	350 ms	46 ms
Return Code	221	221	221	221

Figure 37

How do I identify BYO hubs, switches and routers?

Employees emboldened by their new found home networking skills and commodity networking equipment represent a different bring your own threat to IT. If an employee decides they want another wired port in their cubicle they might plug in an unmanaged, low cost consumer switch available from any big-box store. This would allow them to plug in more than one Ethernet device in their office.

Using Wired Analysis and sorting hosts by Switch Name/Slot/Port arranges the devices according to their connection to the managed enterprise switch. Typically there will be one host device per switch port and each slot/port only occurs once. If a switch port is used by more than one device this indicates a small hub or switch might be attached to the enterprise switch. In Figure 38 the switch `cos_dev_sw3` has multiple devices attached to port 20. Further inspection indicates that this employee has not only plugged a switch into their wall jack, but has used the additional ports to plug in a personal Raspberry Pi credit-card sized linux computer using the MAC address `Rspbry:b827eb-997393`. While the employee might be intending nothing more than doing some lunchtime programming, this device could unknowingly compromise the corporate network.

A more detrimental situation occurs when an employee plugs a residential gateway into the network, unaware that it will act as a DHCP server. In this case both the rogue DHCP server as well as enterprise DHCP will respond to the initial DHCP Discover broadcast message sent as each new device boots up onto the network. In many cases the rogue gateway is located a switch hop away and will respond first, granting a typical private network address in the 192.168.0.x address space. Everything appears normal but the new device cannot communicate on the enterprise subnet.

HOST	ACCESS	SERVER	ALL
cos_dev_sw3.fnet.eng, port 0/1 dtmcospc0114.global.tektronix.net			Dell:001ec9-4ddb3e
cos_dev_sw3.fnet.eng, port 0/9 010.250.000.093			VMWare:005056-760cb8
cos_dev_sw3.fnet.eng, port 0/13 010.250.000.092			VMWare:005056-747749
cos_dev_sw3.fnet.eng, port 0/20 dtmcospc0109.global.tektronix.net			Dell:000bdb-9537b5
cos_dev_sw3.fnet.eng, port 0/20 na008-2k3r2.fnet.eng			Rspbry:b827eb-997393
cos_dev_sw3.fnet.eng, port 0/20 dtmcospc0159.global.tektronix.net			Dell:001422-790c8a
cos_dev_sw6.fnet.eng, port 2/4 ase-sw-cos-eng1			Visual:00a00e-1eafd1
cos_dev_sw6.fnet.eng, port 2/48			

Hosts: 497 Access: 37 Servers: 58 All: 590
Sort: Switch Name/Slot/Port (A-Z)

Figure 38



To quickly identify rogue DHCP servers, the OneTouch analyzer sports an exclusive 2nd DHCP offer detection feature. When a second DHCP address is received during the process of acquiring its DHCP address, over either wired or wireless interface, the OneTouch shows a warning icon on the home screen.

Tap the DHCP server to show the IP address of the server and the address it offered. See Figure 39. If the rogue DHCP server responded first, the 2nd DHCP offer might be the enterprise IP address.

Offer 2	192.168.0.70	--
Offer 2 Server IP	192.168.0.1	--

Figure 39

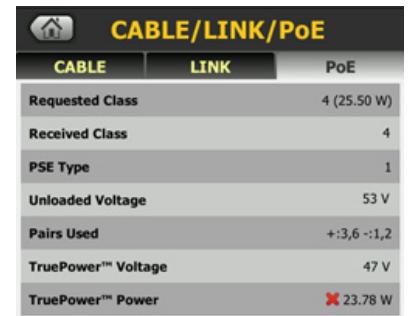
Can I get enough power to my Access Points?

Today's access points draw power like never before as they include two or three radios. The OneTouch AT analyzer and its TruePower™ measurement can measure and load PoE to the IEEE 802.3at limit of 25.5 watts. This lets you verify proper power at the point of install for even the most power hungry APs. PoE is also shrouded in a variety of hardware choices from mid-span power injectors to switch variants and provisioning.

In Figure 40 we see that we can only draw 23.7 watts at the AP location 90 meters from the switch. Moving back to the switch port we can test the power load again to triage between the switch port capability and the patch panel and horizontal wiring. You can also measure the PoE power consumption of an AP inline when using the OneTouch analyzer's capture feature.

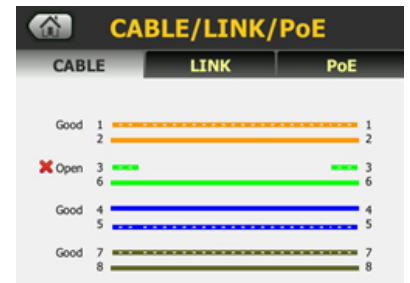
Deploying outside APs connected via fiber? Use the OneTouch analyzer to measure the optical power received through fiber optic links.

Since there is still a lot of wired in wireless, the OneTouch analyzer provides a complete set of cable tests. Understand twisted pair cable using the OneTouch AT analyzer's short/open/cross pair cable tests and TDR length measurements. See Figure 41. Use cable identifiers and IntelliTone™ toning to locate and identify cables as well as Flashing Port.



CABLE	LINK	PoE
Requested Class		4 (25.50 W)
Received Class		4
PSE Type		1
Unloaded Voltage		53 V
Pairs Used		+3,6 -1,2
TruePower™ Voltage		47 V
TruePower™ Power		✘ 23.78 W

Figure 40



CABLE	LINK	PoE
Good 1		1
2		2
✘ Open 3		3
6		6
Good 4		4
5		5
Good 7		7
8		8

Figure 41

What if I need to capture traffic?

Packet capture is the tool of last resort when a detailed, frame by frame view is required to solve a network or application issue. One of the difficulties with Wi-Fi capture is the payload encryption past the MAC addresses requiring decryption by the protocol analyzer. But this only works if weak, non enterprise encryption is used where a simple passphrase or pre-shared key (PSK) can be entered into the protocol analyzer.

Using the OneTouch analyzer's built-in inline aggregating copper and fiber optic TAP to access the traffic running between the access point and switch or WLC, you can capture Wi-Fi traffic in the clear. See Figure 42. The OneTouch analyzer avoids the complexity, time and cost required to configure switch mirror ports or to install standalone TAPs. Line rate hardware filters allow you to single out a station by MAC or IP address, an application such as HTTP by port, or a user group by VLAN. Export the capture file via the management port or SD card to your favorite protocol analyzer (such as Fluke Networks ClearSight™ Analyzer) for decoding and analysis.

When installed inline at the AP, the OneTouch analyzer provides real-time measurement of the Power over Ethernet (PoE) voltage, current and power, so you can quantify the power draw in various AP configurations.

Conclusion

BYOD is here to stay. Most organizations now permit corporate network access by smartphones, tablets, and other smart devices designed for and purchased by consumers for personal and business use. With the multifold increase in devices comes more contention for the air, more network strain, complex policies and provisioning, rogue devices, and user complaints. The Fluke Networks OneTouch AT network analyzer is a unique tool in BYOD management. Its combination of wired and Wi-Fi features used at your desk, on the go, or remotely allow you to quickly inventory, quantify and troubleshoot issues associated with BYOD and the consumerization of IT.

For more information of Fluke Networks' BYOD solutions, please visit

www.flukenetworks.com/BYOD

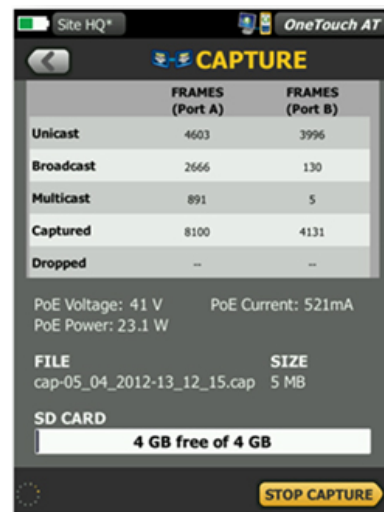


Figure 42



Fluke Networks operates in more than 50 countries worldwide.
To find your local office contact details, go to www.flukenetworks.com/contact.

© 2013 Fluke Corporation. Rev: 01/25/2013 3:45 pm (Literature Id: 4262748)