White Paper: The impact of 802.11ac wireless networks on Network Technicians

802.11n is certainly not dead and whilst manufacturers are still recommending 802.11n deployments, enterprise IT managers should give some thought to and make plans for the eventual implementation of 802.11ac. This new standard brings opportunities to deliver wireless networks to support the future needs of clients especially with the growing demands made on the Wi-Fi network from BOYD smartphones, tablets and laptops. Just like 802.11n, b and g before, 802.11ac promises even greater speeds. 802.11ac will achieve speeds of 1.3Gbs and potentially up to 6.9Gbs if all the new proposed techniques for increasing speed are adopted.

This white paper discusses how 802.11ac is being designed to meet the demands of clients in the future, help you understand the technology, what is likely to happen in the transition from 802.11n to ac and how you can get ready to meet these new demands.

TABLE OF CONTENTS

Executive summary

Future wireless networks must contend with a much higher demand. By mid-2015 it's predicted that more than 50% of smartphones will have 802.11ac hardware included. We must not also forget that tablets can also use 3 to 4 times more capacity of an average smartphone. As a result, there is a growing requirement for higher bandwidth capacity because of applications hosted in the cloud (offsite) and real-time applications like VoIP and Video that are sensitive to loss and latency.

Traffic profiles are also changing; we always expect download traffic to be greater than uploads. Now smartphones and tablets constantly download application updates, receive emails, new adverts, send staying alive pings and have applications that synchronise photos to cloud based storage. In addition, many more mobile devices continuously authenticate and synchronize whilst roaming requiring seamless roaming changes from one access point (AP) to the next.

All this hits the enterprise network as soon as users walk into a building where they have wireless connectivity.

The new 802.11ac IEEE standard provides a platform to meet these growing future needs by implementing significant changes to the 802.11n standard for RF spectrum utilization. The technology improvements greatly improve wireless speeds and throughput capabilities. 802.11ac will operate in the 5GHz band only and will be delivered in two waves.

Wave 1 produces devices that can achieve speeds up to 1.3Gbps using wider bonded channels, increased modulation and up 3 spatial streams.

Wave 2 will produce devices with speeds up to a potential 9.6Gbps with the introduction of even wider channel bonding, up to 8 spatial streams and Multi-User Multiple-Input Multiple-Output (MU-MIMO) technology.

802.11ac promises..

- Increased capacity and higher throughput gained by multiple clients being able to connect at the same time without reducing performance.
- Lower latency, will make higher quality connections to increase the quality of service for real time application including VoIP and video.
- More efficient power usage will mean that there will be less power consumption when data are transmitted.

In planning for future migration to 802.11ac it's important to realize that 802.11ac AP density will be greater than 802.11a/b/g networks to meet user needs of for multiple devices, such as a smartphone, a tablet and a laptop. Planning for sufficient bandwidth for up and downstream is essential. This means you have to plan for capacity and throughput, not just coverage. RF planning and surveying tools such as Fluke Networks' AirMagnet Planner and Survey Pro will aid and simplify the design 802.11ac networks to ensure not just coverage but capacity is designed in from the start.

In the advent of these greater speeds it is important that your existing infrastructure be reviewed and a plan put in place to provide higher speed wired connections to 802.11ac APs in conjunction with greater Power over Ethernet (PoE) capabilities that meet the 802.3at and 802.3af requirements. Once these upgrades have been installed, it will be important to verify these power and throughput capabilities.

Post-installation tests should also be made on the wireless network. Given the gains in speed expected with 802.11ac it would be wise to verify the speed and throughput actually being achieved over the wireless network. 802.11ac devices are likely to mature more quickly in the home wireless router market. This could encourage users to bring 802.11ac devices into the work place to make a convenient wireless connection to their laptop. This would cause a major security breach potentially allowing outsiders to connect to this unauthorised AP. Therefore it's imperative that any devices that you use to detect rogue APs can detect those which support 802.11ac.

Most if not all the measurements discussed above can easily and quickly performed using a hand held tool such as Fluke Networks OneTouch AT Network Assistant that makes these measurements from a wired and wireless client's perspective, saving time and money.

What will 802.11ac deliver?

More and more applications like streaming video, database searches, file transfers, Voice over Wi-Fi, real-time security applications require consistent bandwidth whilst others including backup of large data files, dense environments (e.g., large campus lecture halls and manufacturing floor automation) demand more bandwidth.

The 802.11ac IEEE standard is designed to deliver wireless data networking rates of three to more than six times faster than earlier 802.11a and n networks. 802.11ac products accomplish this by evolving the 802.11n technologies rather than a revolution in technology.

Features include:

1. Increases in multiple transmit and receive antennas, with a maximum of 8 spatial streams.
2. Channel bonding from 40MHz to 80MHz, potentially 160MHz.
3. Transmissions using 256QAM modulation.
4. Multi User (MU) MIMO

However, unlike 802.11n, 802.11ac uses the 5GHz band only. This will make 802.11ac wireless networks more robust as it will not be subject to the interference that plagues the 2.4GHz band caused by Bluetooth, microwave ovens, analog security cameras and DECT phones etc. However, radar will be a consideration when choosing channels in some countries where they broadcast in the 5GHz band.

802.11ac is backwards compatible with the other 5GHz band technologies (802.11a and n). This means that “a” and “n” clients will still be able to connect to APs that have been migrated to 802.11ac. However, there is a cost to this. When 802.11a/n clients exist on the wireless network, the 11.ac clients will be slowed down to a/n speeds.

Early 802.11ac products will typically deliver data rates of 1.3Gbps. With theoretical data rates of up to 9.6Gbps, 802.11ac devices are in a prime position to continue the trend of displacing wired Ethernet connections and increasing the likelihood of all-wireless LAN access networks.

Device/Streams	802.11n 20MHz	channel bonding 40MHz	802.11ac 40MHz	channel bonding 80MHz
Smartphone (one stream)	72Mbps	150Mbps	200Mbps	433Mbps
Tablet (two streams)	144Mbps	300Mbps	400Mbps	866Mbps
Notebook (three streams)	216Mbps	450Mbps	600Mbps	1300Mbps

802.11n vs 802.11ac Data speeds

802.11ac, how does it deliver?

802.11ac uses technologies that have evolved from the 802.11n standard; these new features are wider channels, increased modulation and coding, new beamforming and multiple user (MU)-MIMO.

Wider channels

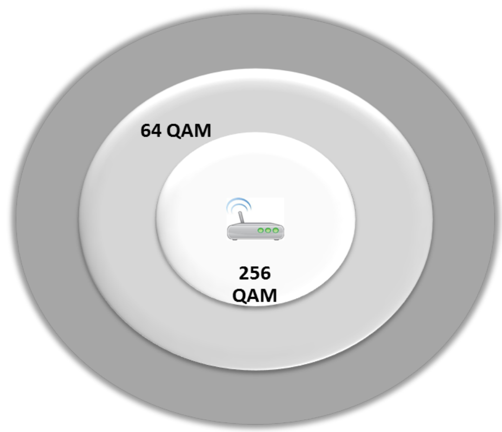
802.11n wireless networks utilise the standard 20MHz channels or 40MHz channels by bonding two 20MHz channels together. Channel bonding is one of the major gains 802.11n used to increase speeds over the other legacy 802.11 networks.

160MHz							
80MHz							
40MHz							
20MHz							
CH36	40	44	48	52	56	60	64

802.11ac has evolved channel bonding; the first products will be released with 80MHz channel bonding. The second wave of products will have the option to use a channel width of 160MHz to still further increase speeds up to a maximum of 9.6Gbps.

Higher modulation and coding schema

802.11n uses 64QAM *(Quadrature Amplitude Modulation)* with a 5/6 maximum coding rate. 802.11ac introduces 256QAM with optional coding rates of 3/4 and 5/6, thereby increasing the number of bits in a single time slice to achieve 1.33 times higher data rates. It should be noted that 256QAM will only provide these rates at short range, approx. within 5-6 meters (15-20 feet) of the access point, but without using more spectrum or more antennas. In addition, it’s likely that 256 QAM will require 5-7dB higher Signal to Noise Ratio (SNR) than that required by 802.11n using 64 QAM.



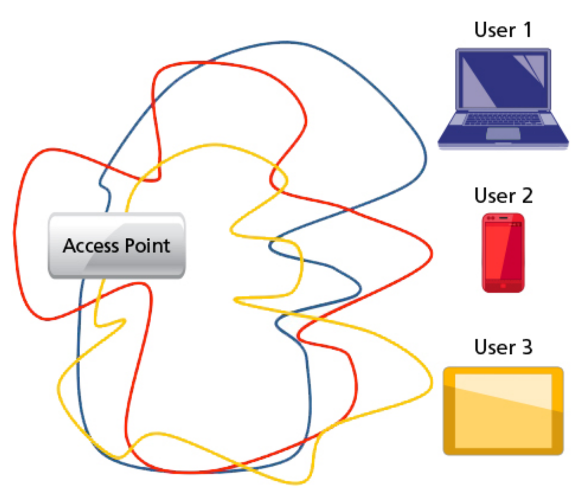
Multi-User MIMO – more spatial streams via more antennae

MIMO is the technology used in 802.11n with multiple antennas for both transmitting and receiving. This effectively multiplies the traffic by the number of antennas. In the case of 802.11n up to 4 transmit and 4 receive antennas could be used potentially quadrupling the data rate, however most 11.n devices in the market place only have a maximum of 3 transmit and receive antennas. 802.11ac APs could have up to 8 transmit and receive antennas providing even greater data rate capabilities. In addition 802.11ac will use Multi User (MU) MIMO which enables simultaneous transmissions to multiple users. The theorectial maximum streams to one client are 4 streams with a total of 8 streams available to multiple users.

Beamforming

Beamforming is a technique first developed with 802.11n which propagates the wireless signal in the direction of the user with the greatest need, improving the performance and coverage instead of transmitting the RF signal to the complete surrounding area.

The diagram on the right shows how Multi-user MIMO used in conjunction with beamforming can transmit to multiple users simultaneously and direct the RF beam to a specific user with each of its antennas.



MU-MIMO and Beamforming

How does 802.11ac affect Network Technicians?

802.11ac sounds like the solution to all of today's wireless challenges. But just like when 802.11n was introduced, there are a number of issues that need to be addressed. With the ability to provide higher capacity and throughput using multiple signal streams, multipath signal propagation and "smart" antenna designs, range and performance will be affected. Consequently, they will also affect AP placement, RF management, optimization and troubleshooting strategies.

With increased wireless capacity comes the requirement to ensure the existing wired infrastructure will meet the demands of an 802.11ac wireless networks capacity to maximise the gains. It's also important to provide enough voltage and power through power over Ethernet to 802.11ac access points with 802.3AT, PoE plus and 802.2.af capabilities.

802.11ac devices are likely to reach maturity in the SoHo (small office, home office) market earlier rather than the enterprise, so expect home 802.11ac wireless routers to be available in your local computer stores very early in the product development cycle. In addition, smart phones will also lead the way on introducing 802.11ac technology. Therefore steps regarding policies and detection should be taken to negate potential security risks of these 802.11ac devices, especially potential rogue wireless router type devices appearing on your enterprise network.

As we discussed earlier, unless you are building a new site you are likely to migrate to 802.11ac so 802.11a/b/g/n devices are likely to exist in the same network. With the backward compatibility that 802.11ac provides, it's important to ensure that any potential ac clients are configured correctly to 802.11ac, otherwise they will slow down other devices.

802.11ac technology cannot be implemented on existing 802.11n based Wi-Fi chipsets, and hence it will require new Wi-Fi client and AP hardware.

Deployment and migration

Many manufacturers are predicting there will be an evolution from 802.11n to 802.11ac rather than revolution, recommending that 802.11n networks should still be deployed in legacy wireless enterprise networks at this time, unless you are building a greenfield site. The placement of 802.11ac access points will also be critical with closer proximity to each other to provide the capacity and throughput required for future proofing. Channel allocation and management will also need to be considered as there will be few 80MHz channels and even less 160MHz channels available. In some countries this will be very difficult with only a single contiguous 160MHz channel available. However, 802.11ac does allow 80+80 MHz channel bonding (discontiguous 80+80) which might help the limited number of 80MHz channels available to make 160MHz channels. For these reasons, it is unlikely we will see significant use of 160MHz channel bonding in enterprise networks.

<table>
<tr><th colspan="2"></th><th colspan="4">America</th><th colspan="4">Europe</th></tr>
<tr><th>Band</th><th>20MHz Channels available</th><th>20MHz</th><th>40MHz</th><th>80MHz</th><th>160MHz</th><th>20MHz</th><th>40MHz</th><th>80MHz</th><th>160MHz</th></tr>
<tr><td>UNII-1</td><td>36,40,44,48</td><td>4</td><td>2</td><td>1</td><td rowspan="2">1</td><td>4</td><td>2</td><td>1</td><td rowspan="3">1</td></tr>
<tr><td rowspan="2">UNII-2</td><td>52,56,60,64</td><td>4</td><td>1</td><td>1</td><td>4</td><td>2</td><td>1</td></tr>
<tr><td>100,104,108,112,116,120,124,128,132,136,140</td><td></td><td></td><td></td><td></td><td>11</td><td>5</td><td>2</td></tr>
<tr><td>UNII-3</td><td>149,153,157,161,165</td><td>5</td><td>2</td><td>1</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="2">Number of non-overlapping channels</td><td>13</td><td>2</td><td>1</td><td>1</td><td>19</td><td>9</td><td>4</td><td>2</td></tr>
</table>

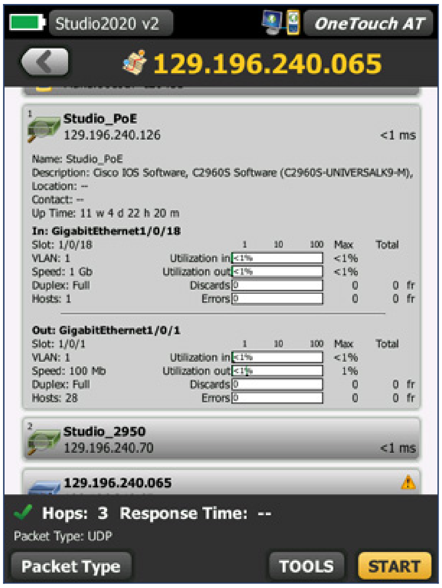
Channel availability

To ensure a good wireless network and design, use a wireless planning and survey tool (i.e. AirMagnet Planning and Survey Pro) to place access points, meet user capacity and data rate capabilities. Please note, when designing for user capacity, plan for three devices per person. With the complication of having multiple 802.11 technologies in one wireless network it is also useful to have mobile handheld tools that can be taken to where the problem exists and provide visibility into the wired or wireless network. This could be a separate tool for the wired network and another for wireless or a combined wired and wireless tool, like Fluke Networks' OneTouch AT Network Assistant.

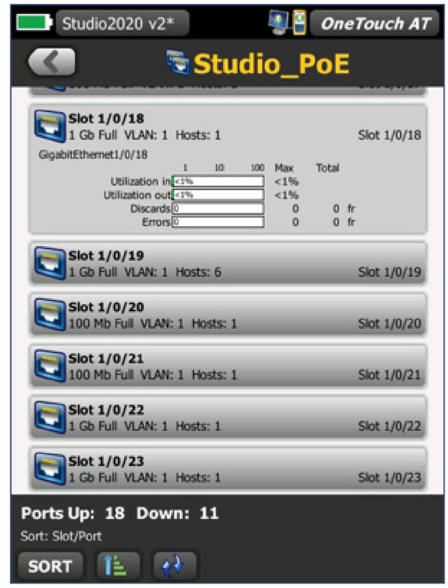
Wired network capacity and power requirements.

Wired network capacity and power requirements.

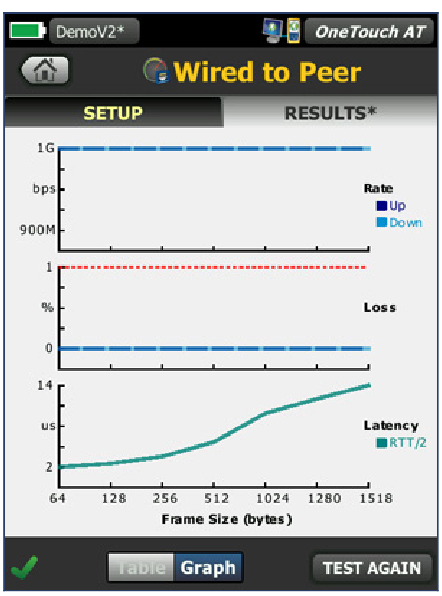
With increased wireless capacity and throughput from 802.11ac comes the requirement to ensure the wired network can support this increased bandwidth. An audit of your switch and router devices should be made to ensure the network paths of 802.11ac APs are capable of providing multiple Gigabit Ethernet connections to client services. Even though 802.11ac APs are more power efficient than other legacy APs, 802.11ac AP wired connections require appropriate 802.3at “PoE plus” power. This makes the verification of wired connectivity and the required class of power available to the AP essential.



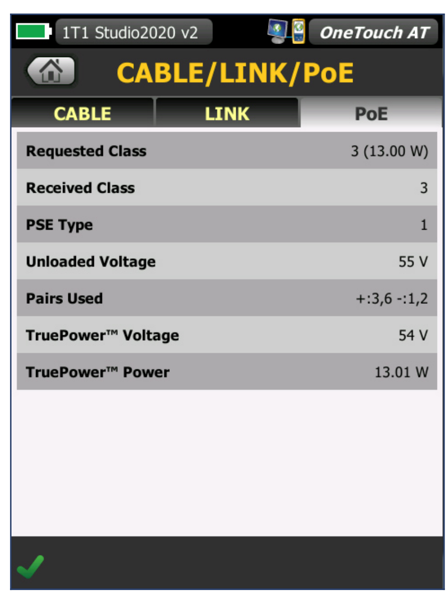
To determine the connection port speeds and headroom in a network path between a client, router or another network periphery device switch by switch; OneTouch AT Network Assistant can run a Path analysis test to show each device in the path and the response time from each device. Further details including the in and out traffic of the ports in the path and the port speed can be gained by selecting a device in the path.



OneTouch AT discovers switches in the LAN between the AP and the Gateway or Router and identifies the speed of each port to determine if capable of supporting 802.11ac speeds.



Ensure performance of the wired link to the AP with the OneTouch AT’s Performance tests. Measure upstream and downstream throughput up to 1Gbps as well as loss and latency.

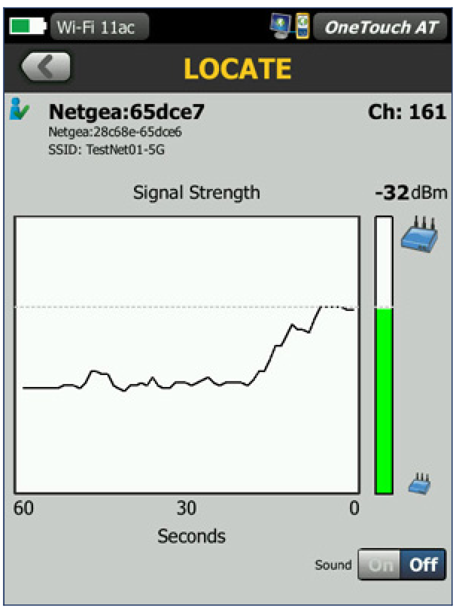


802.11ac APs can be tested for wired connectivity and PoE capability with OneTouch AT. On connecting to the AP a test is automatically run which displays the TruePower™ available under load at the AP’s location.

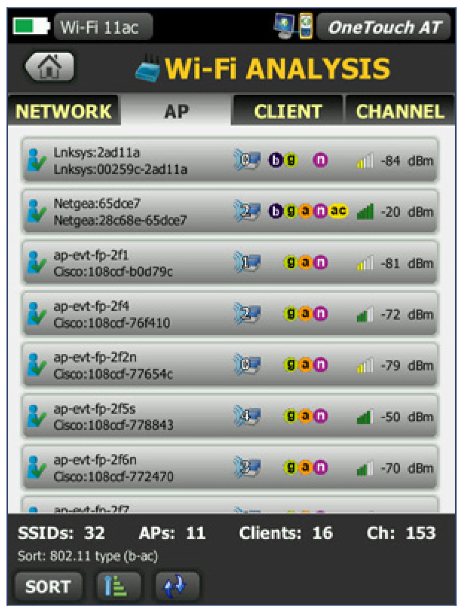
Security

The small office/home office 802.11ac device manufacturers will likely be ahead of the game, launching 802.11ac wireless routers. As discussed earlier, these devices are highly likely to find their way on to enterprise networks. Users reading the marketing blurb on 802.11ac wireless router boxes in their local PC store will see up to 1.3Gbps speeds advertised. This will prompt them into believing they can use these devices to make a convenient 1Gbps wireless connection from their laptop into their workplace network. Unfortunately, they could also be causing a major security leak on their corporate network. To ensure this does not happen on your network, a 24x7 intrusion detection system (IDS) or intrusion prevention system (IPS) that can detect 802.11ac rogue devices should be used. However if you do not have one of these systems you can use a handheld wireless tool that can discover 802.11ac, categorize and locate 802.11 ac rogue devices. If you do have such a system, the portable nature of the OneTouch AT makes it the go-to tool for finding the physical location of the offending device.

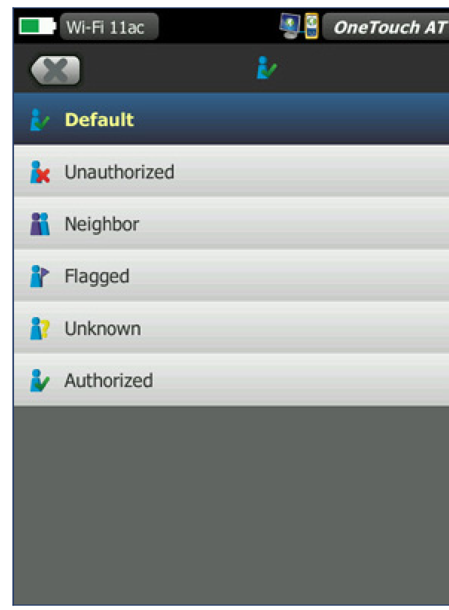
The OneTouch AT also features a unique “cross-linked” discovery which shows the wired location (port/switch) of AP’s discovered on the wireless side of the network. This facilitates the ability to quickly disable network access for unauthorized devices.



Once discovered, a 802.11ac access point can be physically located based on its signal level. Using the OneTouch AT Locate tool, track down a device to mitigate a rogue security threat or to find an access point to perform move, add or change operations.



The OneTouch AT is able to detect and classify 802.11ac capable access points by decoding specific information in beacons. Discovered 802.11ac access points are reported under the AP tab as well as in Network, Client and Channel filtered access point lists and marked with an 802.11ac icon. 802.11ac is included in media type sorting so a user can raise the visibility of detected 802.11ac access points in the list of discovered access points. This can be used to quickly identify rogue devices or review a newly deployed network of 802.11ac access points.

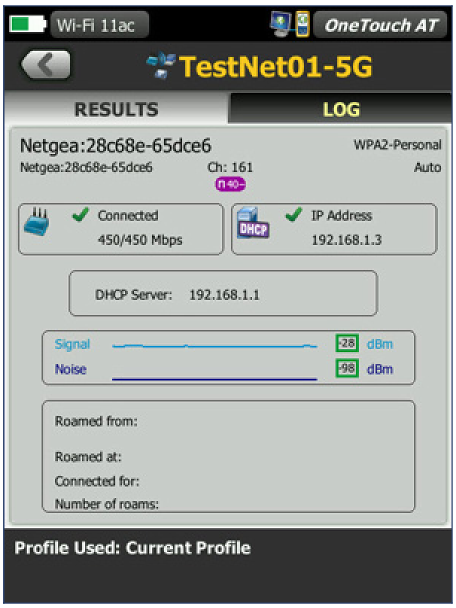


By allowing you to tag and name known AP’s on your network, the OneTouch makes rogue detection quick and easy.

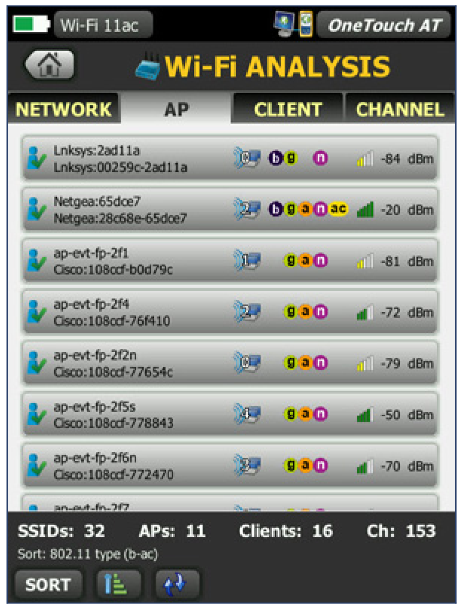
Connectivity, troubleshooting and optimization

Once 802.11ac wireless access points have been installed, whether in a hybrid legacy 802.11a/b/g/n network or an 802.1ac greenfield site, it's important to verify connectivity and that 802.11ac capable clients are actually connecting using 802.11ac settings to get the additional speed benefits. First-generation 802.11ac AP products will have to be matched with peer 802.11ac clients. This means that a three-stream, 80MHz channel connection can only be supported between matching AP/client pairs.

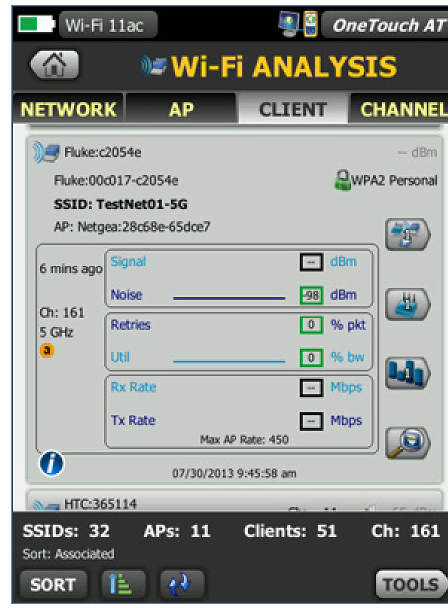
If clients are connected using 802.11a or even b or g, not only will they suffer slower speeds, but they will also make the connections of other users slower.



802.11ac is backward compatible with 802.11a/b/g/n supporting connectivity of legacy clients. Verifying the ability to link and gain network access is an important part of solving connectivity issues. OneTouch AT has a connect tool for 802.11ac networks and access points. In addition to this results screen, a complete log of the connection process is shown under the LOG tab, making it easy to identify where in the association, authentication or IP address process the problem exists.



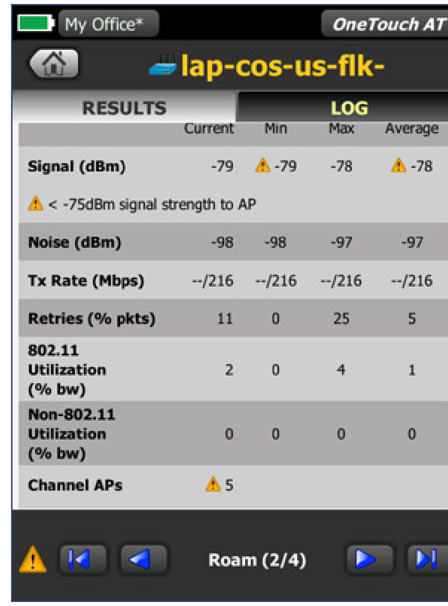
OneTouch AT can discover 802.11ac APs and provide AP details, classify .11ac APs with regards to authorization status, locate 802.11ac APs, connect to 802.11ac networks, discover associated clients and client details, analyse 2.4 and 5GHz channels, capture 802.11ac management and control frames, verify client connectivity and measure the end user experience.



OneTouch AT will report all clients associated to an 802.11ac capable access point that it sees using the network. This client information makes it easy to spot those clients that should be connecting using 802.11ac, whether they are 802.11a, b, g, n or ac clients.

Roaming

Seamless roaming between wireless access points is now accepted as an everyday requirement with the ever increasing number of BYOD's (Bring-Your-Own Devices) in the enterprise network. In addition, many applications including data, voice and video running on these mobile and other devices depend on a persistent network connection; even a momentary loss of that connection can disrupt the communication and negatively impact a user's productivity. Wi-Fi roaming tests verify clients can move from one AP to another AP within the same network or SSID without losing their connection. Roaming transaction details for clients including PCs, phones, and other mobile devices should be examined for signal level, noise, channel number and retries as these determine if network coverage, congestion, or interference are the cause of bad roams. These parameters can be captured and reviewed by Wireless Analyzers i.e. AirMagnet WiFi Analyzer and some advanced handheld analyzers such as the OneTouch AT.

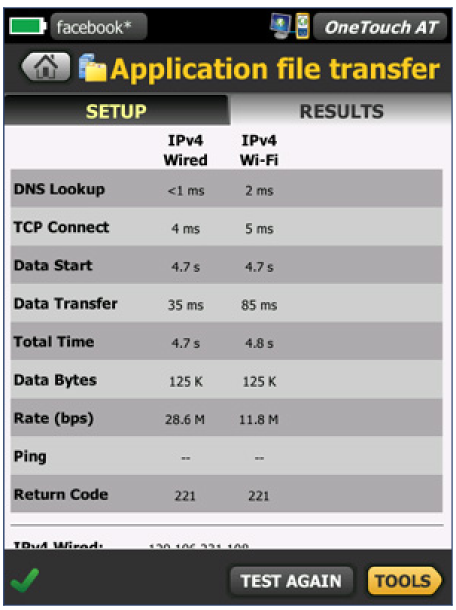


OneTouch AT provides a summary of the Wi-Fi connection and local network health. Roaming details include AP MAC, connected channel security method used to connect and network health statistics. These metrics are key indicators of network coverage, congestion or interference issues that can impact client connectivity and performance. For each statistic, the current, min, max and average values are shown and a warning will be reported for measurements that fall outside the respective threshold/limit.

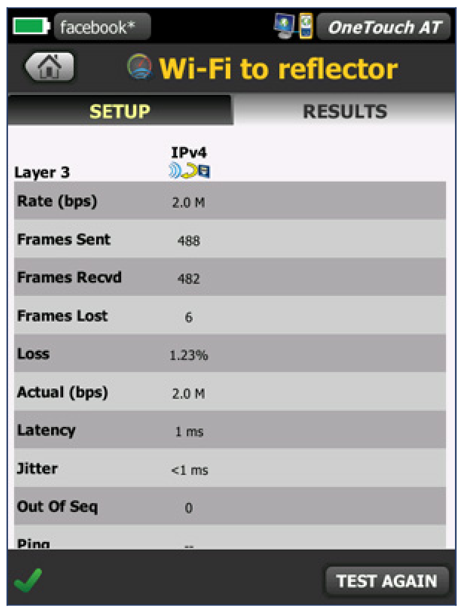
Throughput and service availability

The ultimate goal of designing and installing an 802.11ac network is to meet the required user capacity, throughput and network response times. By achieving these design criteria, you will provide users with a good service to all their applications. This may be streaming video, VoIP, downloading large files, email etc. So, the ability to measure these parameters and verify performance would be a great advantage to understanding what's happening in the path between the client and the server or application. These measurements should be made through the LAN to the network core, then through WAN links to cloud services and remote office buildings, as a client. The resulting comparison between the wired and wireless results provides valuable information to determine if the problem is unique to the wireless network.

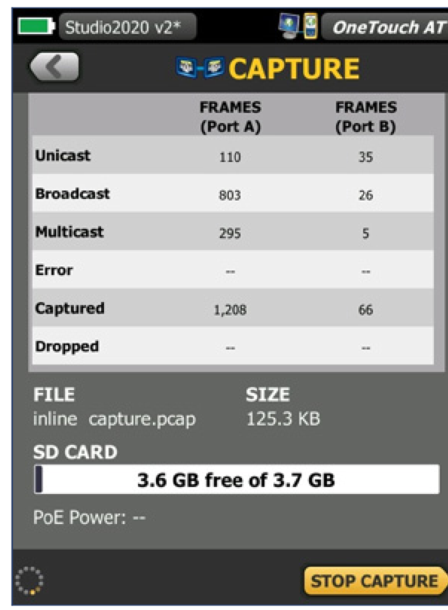
After making these tests, the results should be examined to verify good throughput and response times. These tests will vary from network to network and from where the measurements are made to and from. Regular testing of these parameters from a variety of clients to different services will help you to understand what is normal, making it easy to detect when there is a problem. If the results of the tests are deemed to be good and clients are still complaining about the response, then it may be necessary to capture the trace between the client and the access point (inline) for escalation or further analysis.



Verifying applications' connection speed and throughput could not be easier with OneTouch AT. A variety of application tests including FTP, email, Video and Web connectivity can be included in a profile, then tested simultaneously from a wired and wireless connection, providing a direct comparison between both access methods.



OneTouch AT has the capability to make throughput testing through the wired or wireless conection to either another OneTouch peer or a LinkRunner AT. This powerful feature enables network technicians to quickly and easily verify traffic throughput capabilities through to the core network, servers, and remote sites.



In the situations where no anomalies can be found in the results of an application or service test, but clients are stil complaining about application throughput and response times. OneTouch has the abilty to connect inline with the AP and the network or on a wireless connection to collect packets for escalation and further analysis with a Protocol Analyzer such as Fluke Networks ClearSight, an application-centric analyzer that provides quick answers to application performance problems.

Summary

With the advent of the 802.11ac standard, network technicians, engineers and IT management should make plans for how they will implement 802.11ac in their network site by site. Considerations of the way this new technology will be implemented and the changes required in existing enterprise networks should be discussed, thought though and a plan made. Special considerations should be made to user density, as this will affect user capacity and the throughput required. This will drive access point placement and a need to upgrade existing wired infrastructure for 802.3at power and multiple gigabit connections to wireless access points. With 802.11ac home wireless routers already becoming available, network security should be reviewed to ensure rogue 802.11ac devices can be detected. Last but not least, verify wireless roaming capabilities, user application and server response time to understand what's normal and to understand what gains have been made from any investment of 802.11ac installations.

About OneTouch™ AT Network Assistant

The OneTouch™ AT Network Assistant is an automated all-in-one tester for understanding end-user Gigabit Ethernet and Wi-Fi network performance. Combined twisted pair, fiber optic and Wi-Fi testing resolves countless problems. Automated testing with pass/fail analysis speeds problem identification. An AutoTest profile standardizes troubleshooting and performance validation practices. Wired and Wi-Fi end-to-end path performance measurement to a remote peer or reflector documents SLA compliance. Inline VoIP analysis troubleshoots IP phones in real-time and measures call quality. Wi-Fi and inline wired packet capture streamlines collaboration and problem escalation. Discovery and analysis provides visibility into wired and Wi-Fi networks. Comprehensive cable to server testing isolates the problem root cause.