KOMODO SYSTEMS

NETWORK MANAGEMENT, YOU CAN'T MANAGE WHAT YOU CAN'T SEE

Understanding user experience metrics and employing them to improve network performance is a new "best practice".

SCHEDULE DEMO
www.komo.do/demo

komodo® SYSTEMS

Komodo Systems
6936 South Promenade Drive, Cottonwood Heights, UT 84121
855-WIFI-066 (855-943-4066) | **www.komo.do**

A VIEW FROM THE **USERS' PERSPECTIVE**

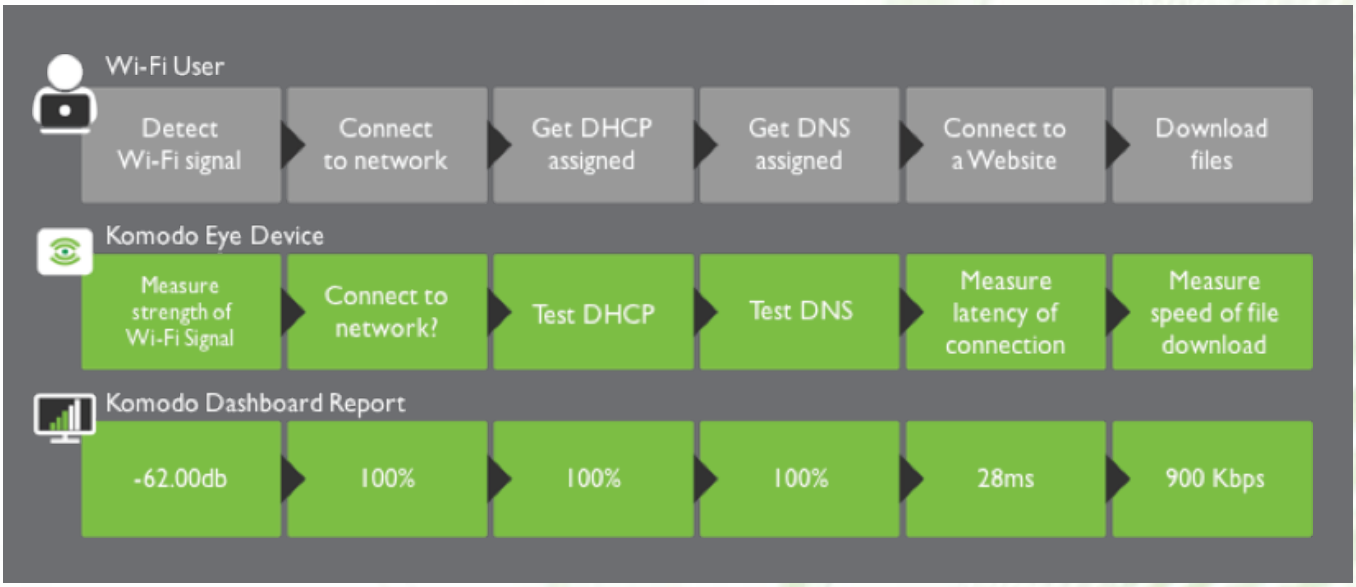
Komodo Systems – troubleshooting common Wi-Fi Network problems

Wi-Fi networks are notoriously difficult to troubleshoot, simply because it is difficult to see what an end-user is experiencing when they encounter a problem. Komodo Systems addresses this by simulating the end-user with multiple devices – Komodo Eyes. The Eyes give the network manager an ongoing view of users' experiences on a Wi-Fi network or LAN, making triage, troubleshooting, and resolution much simpler. Although the Komodo Eye gives you a user-centric view, it often requires a network-centric intervention to resolve an issue. When Komodo Eyes detect a user problem or poor user experience, there are several common issues that frequently crop up and relatively simple network interventions to resolve them. This whitepaper describes the common instances where users have poor Wi-Fi experience, and typical interventions available to network managers to resolve them.

How Komodo User Testing Measures a Network

Komodo Eyes test networks by following the same workflow that a client device follows when it connects to a network, accesses the internet, and downloads files. At each step in the workflow, Komodo captures metrics related to that step, and reports them back – running through the same set of tests every 5 minutes. When a failure, or poor performance is measured, the manager is notified. The rest of this whitepaper describes the most common failures and problems encountered at each step, and common ways to address them.

Komodo and User Connectivity Workflow



Komodo and User Connectivity Workflow

Komodo Systems
6936 South Promenade Drive, Cottonwood Heights, UT 84121
855-WIFI-066 (855-943-4066) | **www.komo.do**

Airspace Scan – finding the right SSIDs and Access Points

Frequently the airspace being managed by a network professional is congested – numerous SSIDs and APs are broadcasting in the space. The Komodo Airspace Report (see Reports=> Airspace Report) shows what other SSIDs and BSSIDs are broadcasting in the airspace and their signal strength and channel. The scan may reveal common problems with Wi-Fi networks:

1 **The desired SSID is not broadcasting on all managed APs in a network.** Frequently, a desired SSID is not active on all APs in a facility, or an installed AP has not been configured. This may cause problems with signal strength and association, and is typically revealed when the airspace scan shows which APs are broadcasting each SSID. This is easily resolved by activating the desired SSID on the desired AP.

2 **An old SSID or default SSID is still broadcasting.** In many cases, an old, or decommissioned SSID is still active on some APs. This may cause channel congestion or may cause confusion for users that connect to the old SSID on one access point and then move to another location in the facility, where the APs are no longer broadcasting the old SSID.

3 **Channel congestion** – if too many other SSIDs, of sufficient signal strength, are broadcasting on the same channel, there may be impacts to association and bandwidth. The Komodo Airspace Report shows the number of conflicting SSIDs and their signal strength. Selecting the most available channel for your SSIDs reduces airspace congestion.

4 **Rogue APs or SSIDs** – in some facilities users may set up rogue networks without the knowledge of network management. The Komodo Airspace Report identifies these rogues within a minute of them coming on line and can assist in identifying them. The reporting BSSID will reveal the manufacturer of the AP, and signal strength information can help identify the location of the rogue.

Sample Airspace Report

Access Points being tested (2/7)

Komodo Eye Device test assignments and their airspace details

DEVICE	MAC ADDRESS	VERSION	BSSID	STRENGTH	ESSID	COUNT SSID	CHANNEL	CONFLICTS	ACTION
B.C. - 301	60:e3:27:a2:97:62	tl-wr710n-2.0.34-dev-komodo	a4:13:4e:26:29:b9	-32 dBm	Brigham	24 other(s)	7	1 conflicts(s)	Edit Configure
B.C. - Laundry	c4:e9:84:34:17:f2	tl-mr3020-2.0.35-dev-komodo	a4:13:4e:26:29:b9	-54 dBm	Brigham	23 other(s)	7	1 conflicts(s)	Edit Configure

Possible rogue SSID and Access Points

Signal strength -65 dBm or better and not a known SSID

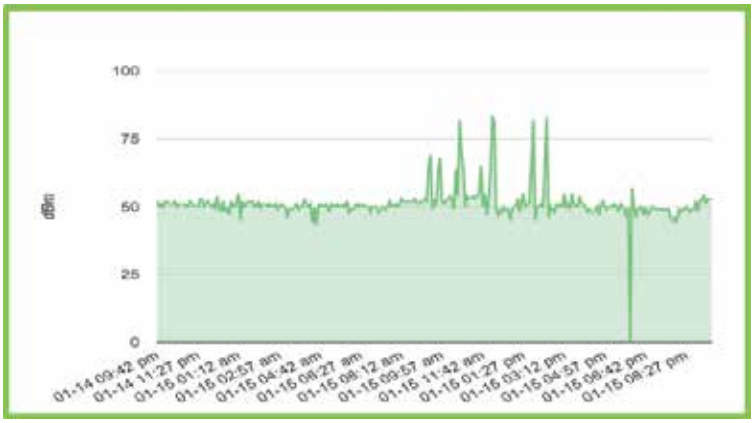
BSSID	STRENGTH	SSID	CHANNEL	COUNT DEVICES	ACTION
20:25:64:E9:19:C9	-53 dBm	*	6	2	Ignore Add SSID
5C:8F:E0:69:D9:52	-57 dBm	scottfamily	11	1	Ignore Add SSID
6E:8F:E0:69:D9:52	-65 dBm	xfinitywifi	11	1	Ignore Add SSID
54:BE:F7:AA:B1:21	-54 dBm	*	1	2	Ignore Add SSID
C4:27:95:CD:68:05	-63 dBm	HOME-6805	1	1	Ignore Add SSID
C6:27:95:CD:68:07	-64 dBm	xfinitywifi	1	2	Ignore Add SSID

Signal Strength
Normal Range: -20dbm to -65dbm
Too Weak: -65dbm to -100dbm

Signal strength typically won't fluctuate. If the client device and the AP are stationary, and nothing moves in between to block or deflect the signal, the signal strength should not change over time. If signal strength worsens to -65dbm or beyond, user performance may be compromised. If you see signal strength change over time, there is something going on in your airspace that you should be aware of. The most common scenarios our customers encounter are:

1 **The AP automatically adjusts signal strength and beam forms to clients.** Typical of more recently launched enterprise APs (we have most recently seen this with Aruba) the access point will adjust the signal strength, directing signal to where the clients are. Opinions of these APs vary between network managers. Some appreciate the ability of an AP to auto-select the optimal channel and direct signal to clients. Others find the auto-adjustments problematic and unpredictable and prefer to turn off this functionality upon installation.

2 **Something is moving through your airspace and blocking the signal.** Metal furniture, vending machines, containers of liquid, and even large numbers of people (which are, after all, large containers of liquid!) can block or deflect Wi-Fi signals. An example would look like this:



Notice the spikes in the middle of the day? This site is an office that had recently added a significant number of new employees. As these people moved through the office space, they blocked the Wi-Fi signal, causing the signal strength to spike to -75 dBm which makes it difficult for user devices to connect.

3 **The power settings are turned down on the AP radios.** It is often a best practice to turn the power, on a set of APs, to the lowest setting for the desired coverage area. This prevents overlap on a heat map, and ensures that only a relatively small number of users can attach to the AP – preventing congestion, and improving the user's experience. However, this can inadvertently create dead spots in a facility. See here:

In this case, at 8am on a Friday, the network manager turned down the power settings on his Ubiquiti APs to redeuce overlap. This impacted signal strength throughout the facility – in most cases the user experience wasn't effected. However, there were several rooms where the weakened signal strength negatively impacted users. In the graph above, the signal strength went from -55dbm to -70dbm. The Komodo Eye was still able to connect, but its negotiated bitrate was much lower and users experienced a deterioration in download speeds. Seing this, the network manager quickly reversed his changes, and the performance improved.

Association (pass/fail)

Failure to associate is typically a result of:

1 The client device having the wrong password or the wrong encryption type.

2 Seeing a captive portal that prevents association. This can be addressed quickly by whitelisting the MAC address of the Komodo Eye, if desired.

3 The AP not broadcasting the SSID (see above in "Airspace Scan")

Occasionally this is a more complicated issue where the Komodo Eye is trying to test multiple SSIDs and then is reporting over the LAN. Some networks will flag this as suspicious behavior and attempt to block association over one of the wireless SSIDs. This can be remedied by setting the devices to backhaul over the WAN. Go to Configuration -> Komodo Eyes and click on the "Wireless" button for the device in question.

DHCP (pass/fail)

Failure to DHCP is typically related to one of the following:

1 DHCP lease time set too long. DHCP lease times of more than 8 hours (28,800 seconds) can result in all IP addresses in a network being consumed by a rush of users and client devices. You can check DHCP lease time by going to "Network Status => Wireless Network => Historical => mouse over the DHCP Log to see lease time.

2 DHCP IP pool is empty. This will happen if too many clients have attached to a network and used up the pool of IP addresses. Check your controller to see if your IP address pool is empty and to see how many clients are attached to your network. This can be resolved by either reducing DHCP lease time (see above) or increasing the pool of available IP addresses.

3 Two or more dueling DHCP servers. If there is more than one DHCP server on a network, client devices can get confused when more than one lease is being handed out, or more than one IP address is being handed out. In these cases DHCP will succeed, but DNS and other downstream tests may fail frequently. Follow the steps above to see which DHCP server the device is seeing. Having only one DHCP server on the network typically resolves this issue

4 DHCP server is down or unavailable. If the DHCP server is down or unavailable, DHCP will fail. Check your DHCP server to see if it is still functioning and handing out leases.

DNS (pass/fail)

DNS failures are rare and typically related to the following:

1 Dueling DHCP servers (see above – this will result in failed DNS).

2 Security settings blocking outbound access to the internet. Occasionally corporate networks are set to prevent unauthorized devices from accessing outside websites. Check your controller and security settings to ensure that each network is set correctly.

3 Network or ISP DNS server is down. This is rare, but can happen. Running the Komodo LAN test can help determine the source of the DNS failure. If the LAN test fails DNS, then the ISP is the source of the failure. If DNS succeeds on the LAN but fails on the Wi-Fi network, there is likely a misconfiguration on the local Wi-Fi network or access point.

Latency

Normal Range: 2ms to 50ms

Problematic: 50ms or greater. At 50ms, gaming, voice applications, and other high bandwidth, real-time communications will be poor. At 100ms, video streaming will be impacted, and over 500ms the network will be essentially unusable – even to web browsing.

High latency on a network is problematic because it can drastically impact the user experience, regardless of the bandwidth available on a network. A high bandwidth network with high latency will still deliver a poor end-user experience. When testing latency, the Komodo devices ping a pre-determined web address. We suggest selecting a web address that is pertinent to the users on your network. High latency on a network typically results from:

1 **High baseline latency at the ISP.** Sometimes your internet service provider does not provide optimum routing for your web traffic. In this case, the baseline latency will regularly be 50ms or higher. This is the case if high latency is detected in both the Wi-Fi and LAN tests. The traceroute function can help you pinpoint exactly where the latency is being introduced.

2 **High baseline latency on the Wi-Fi network.** If all devices on a Wi-Fi network are reporting high latency, but the LAN is not, there is typically a filter, firewall, or security policy on the network that is slowing web traffic. Viewing Komodo's traceroute will tell you where the latency is being introduced.

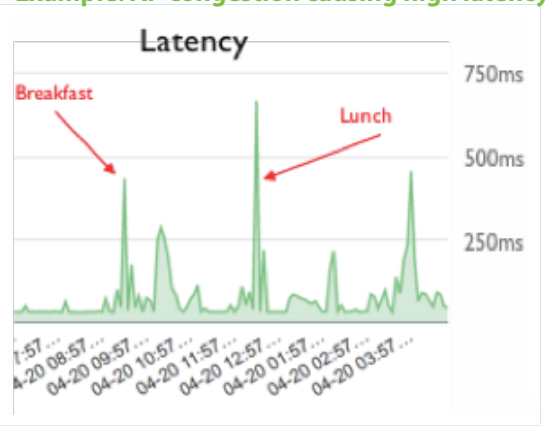
Example – LAN with high latency – hop 11 is adding 90ms of latency

3 **Latency spikes on a network.** Spikes in latency typically occur during times of heavy usage. When there is insufficient bandwidth into the building, or when there is congestion at an access point, temporarily high latency results. In the first case, the ISP circuit is not sufficient to accommodate usage on the network. In the second case, the ISP circuit is sufficient but the individual access point cannot accommodate all the users and traffic.

Speed and Performance

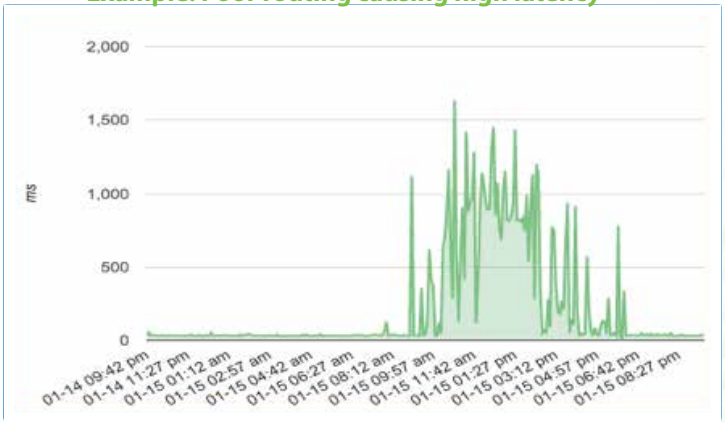
When measuring internet speeds, network managers are accustomed to thinking about the total bandwidth of the ISP circuit. However, the average user on a network almost never uses the entire bandwidth of a circuit, even when streaming videos. For normal web browsing or email, the average user needs a small fraction of their internet pipe.

Example: AP congestion causing high latency



In this case a restaurant with one AP could not effectively handle user traffic during peak hours. When there are no users on the network, the latency is low. However, during peak meal-times, when there are users on the network, the AP cannot handle the traffic without severe latency. The solution, in this case, is to add more APs or to replace the existing AP with a higher-capacity model.

Example: Poor routing causing high latency



In this example, a software company's office is experienced severe latency during working hours due to inefficient the ISP routing. With latency spikes over 1000ms, the network was essentially unusable during the day. A quick call to the ISP rectified the situation.

Although Komodo does measure total available circuit bandwidth (see "Performance" on a room card), this information normally provides very little information about the end-user's experience. However, the ISP circuit speed is greatly impacted by latency on a network – a high bandwidth network with high latency can provide a much worse end-user experience than a low bandwidth network with low latency. To more accurately measure end-user experience, the Komodo device downloads a small file every 5 minutes – a file the size of a webpage image – to test speeds available to an end-user. Since the file is small, speeds are typically much lower than the overall circuit. The "Performance" score is the overall available bandwidth of the circuit, while the "Speed" score is the bandwidth available to one individual user surfing the web. These smaller files are typically much more sensitive to network fluctuations, and will show variations in network performance more readily.

Download speed tests typically fail or demonstrate poor performance when:

1. **There is congestion on an access point.** If there are too many users, or are too many high-bandwidth users on an access point, the Komodo test will show a dramatic drop-off in speed. This is usage dependent – when the high-bandwidth users drop off, speeds will recover. This is typically resolved with a high capacity access point, or more access points covering the affected area.

2. **Insufficient bandwidth** – the ISP circuit is unable to accommodate the usage in a building. If all Komodo Eyes in a building are showing a drop-off in speed, (and APs are otherwise functioning, with no fluctuation in signal strength) then likely this is a problem with ISP bandwidth. A Komodo LAN test will confirm this. Again, this typically self-resolves when user traffic drops. A typical network will see speed fluctuations: improving during the night (low-usage times) and then deteriorating during the day (high usage times). This can be addressed by increasing ISP bandwidth.

3. **Filtering or security settings preventing access to outside points.** Occasionally a security setting or firewall will block outside access to the download file. This will appear as an intermittent speed test failure or you will see all the other tests succeed, yet the speed test fails.

Review –

End-user testing is critical for most operational systems and is especially useful in Wi-Fi network management. The quality of the end-user experience is the critical metric needed to truly understand and manage a wireless network. Understanding user experience metrics and employing them to improve network performance is a new "best practice". Previously this perspective was only available to network managers through labor-intensive site visits. This whitepaper leverages the experience of dozens of network managers, illustrating how to interpret the use end-user experience and make effective improvements to your network. The principles illustrated by these examples should help network managers take advantage of the new availability of end-user data on an ongoing basis.