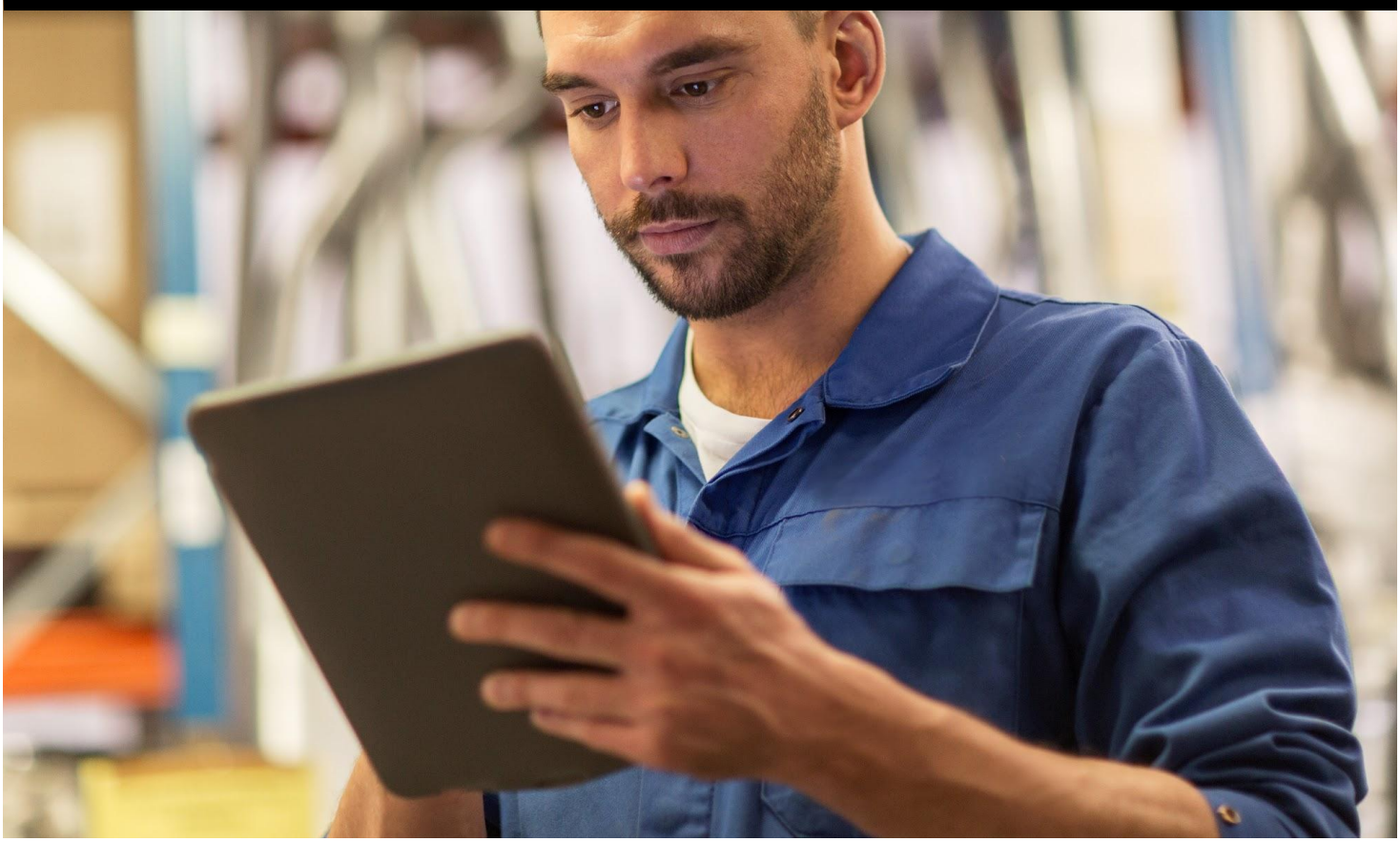
The Ultimate Guide to Troubleshoot WiFi Networks with the OSI model

2020

tanaza



Overview

Deploying a robust state-of-the-art WiFi network that allows delivering high performance and reliability has turned out to be a challenging task for many enterprises. Wireless networks can be expensive and complex to set up and implement; thus, organizations, more than ever, seek assistance from MSPs.

Rightful, having a cloud-managed WiFi solution that proactively pinpoints performance issues before your customers know they exist, has become a necessity. Nowadays, network administrators need to be able to troubleshoot issues right away, remotely, and fast.

Lets deep dive into how to troubleshoot WiFi networks.

Best practices to outline problems with WiFi networks

Before attempting to solve any issues with WLANs is crucial to understand the root of the problem and gather information about the situation by answering the Five Ws questions (who, what, when, where, why), to outline the issue and define an action plan.

Identify the issue by asking the right questions to your customer.

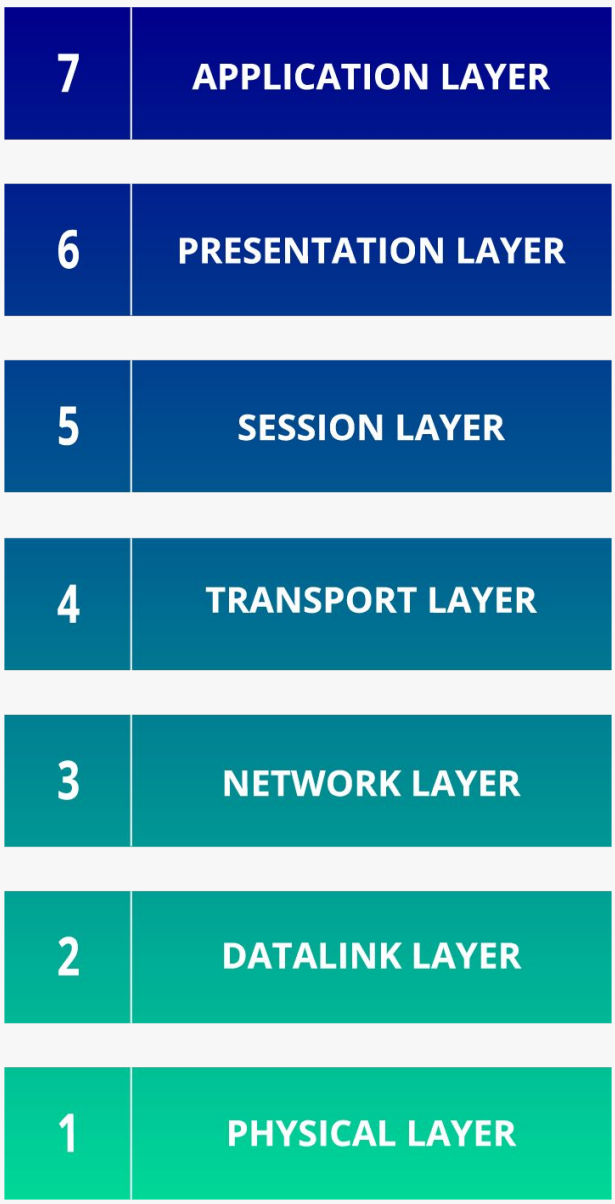
1. **What** is the problem the customer has? Is it a slow connection to the Internet or no Internet access at all? Or does the Internet connection drop randomly?
2. **When** is the problem happening? All the time, at certain times in the day, once in a while? Timestamps are key! Check the access points log files you are monitoring.
3. **Where** is the problem happening? Is the problem described in question one happening in one area? Multiple areas? Is it campus-wide. By asking this question, the problem can be isolated to a specific access point or area.
4. **Who** gets affected by this problem? Does the problem affect one client or many client devices? If it affects many devices, it might be a deeper issue; however, if it's affecting one client, it might be a problem with the device itself and not with the entire WiFi network infrastructure.
5. **Why** is the problem happening? Mostly it could be associated with changes carried out by the customer. Understanding if the customer did any change to the WiFi structure that might have triggered the problem is crucial.

Once you have gathered all the key information from your customer, it’s time to troubleshoot the WLANs, layer by layer.

How to Troubleshoot WiFi networks with the OSI model.

At Tanaza, we like to take a structured approach when it comes to troubleshooting our own WLANs. We use the OSI (Open Systems Interconnection) model as a framework for troubleshooting network problems.

The OSI model is a conceptual model that enables different communication systems to "talk" in the same "language" using standard protocols. This universal language for computer networking splits up the communication system into seven different layers, each one stacked upon the last.



The OSI model helps to break down an issue and isolate the root of the problem. Ideally, we suggest taking a layer bottom-up approach. When it comes to WLANs, most of the WiFi problems happen in the first two layers of the OSI model. So, if the issue can be narrowed down to one specific layer, you can save time and avoid needless extra work.

In this guide we will cover troubleshooting WiFi Networks at Layer 1 and 2 of the OSI model.

Layer 1

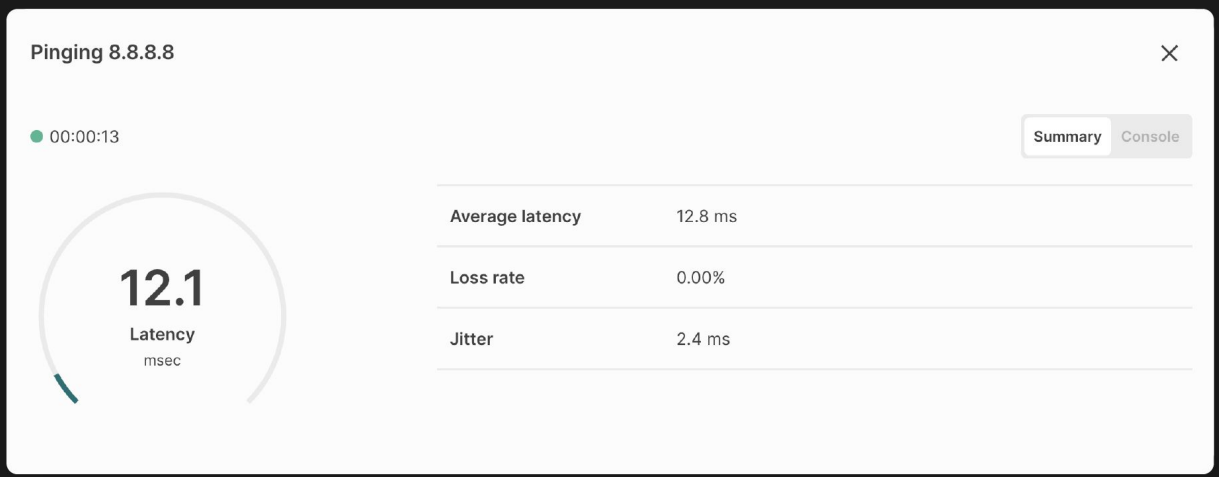
The layer 1 of the OSI model, includes the physical equipment involved in the transmission and reception of data, like connectors, cables, switches, and fiber. In this layer, the data is converted into a bitstream, a series of 1s and 0s. That means the physical layer of devices, by default, must agree on code and modulations; thus, the 1s can be separated from the 0s on both devices.

As a rule of thumb, WiFi (802.11) operates at the first two layers of the OSI model. In other words, the physical layer and the datalink layer. Broadly speaking, **Physical Layer issues can be split into two main groups: outage and performance issues.**

Investigating **outage issues** is the easiest one. Network admins can start by simply checking that all the equipment is connected correctly, and access points, switches, cables, and gateways are turned on and online.

On the other hand, when delving into **performance problems**, it's crucial to have the right tools to diagnose degraded performance. An easy and fast way to understand performance issues is by pinging devices to know whether the target device is active, the network path between source and destination is right in both directions, and also to measure the packet round trip time to determine latency and jitter levels.

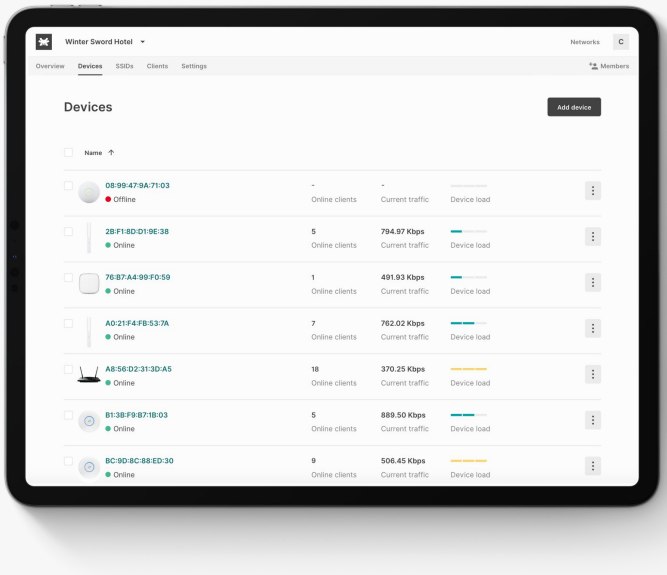
The **Tanaza software** has an embedded **ping tool** that allows network admins to perform routine ping tests. After pinging a device, the tool displays the ping results through dynamic diagrams. These graphics allow users to get a quick overview of the network situation in a fast and organized way, while at the same time pointing you in the direction of what's causing the Physical Layer problem.



Layer 1 - continuation

Also, as part of the check-up, take a quick look at the **configuration of the device's drivers and the access points' configuration**. Commonly the main reasons for a breakdown in the connectivity. First-generation radio drivers and firmware are notorious for possible bugs, which often causes connectivity issues with brand-new access points. Ensure all client devices, whenever possible, have the latest drivers installed and ensure that all access points are upgraded with the latest operating system.

The **Tanaza WiFi cloud management platform** allows network admins to update the access point firmware of all cloud-managed access points in bulk without the need to reboot the devices and from remote. With each firmware release, Tanaza delivers turnkey features, patch vulnerabilities, and drive security and stability, to empower your devices.



Radio frequency signals can cause another potential performance problem. An outside entity causes noise that interferes with the signal or dataflow across the network, affecting not only the performance but also the coverage of the WLAN, i.e., a microwave interfering with the WiFi signal.

High Power. Having the access points transmitting at full power, particularly for indoor deployments, might lead to oversized coverage, increasing co-channel interference and roaming issues, like sticky clients. So take a notch down in the access point power.

The problems mentioned above can always be avoided with good WLAN design before deployment. Most of the issues that appear because of inadequate WLAN design are coverage holes due to access points misplacing and antenna orientation and co-channel interference. WiFi should be designed for capacity and air time, not for coverage.

Layer 2

The second layer of the OSI model is the data link. This layer helps to transfer data between two devices on the same network. For instance, the data link layer takes packets from the network layer and breaks them into frames. The data link layer is responsible for flow and error control in intra-network communication.

The data link layer has two sublayers: the Logical Link Control (LLC), which interprets electricity, light, and WiFi into 1s and 0s that become the data packets. The other sublayer is the Media Access Control (MAC) layer, accountable for moving data packets to and from one Network Interface Card (NIC) to another across a shared channel. Thanks to the MAC protocols used in the sublayer, the signals sent from different stations across the same channel do not collide.

WiFi radios talk via 802.11 frame exchanges at the MAC sub-layer of the data link layer, then the next layer to look into when troubleshooting is layer 2 of the OSI model.

Retransmissions

The most common problem in layer 2 is retransmissions that happens at the MAC sublayer. Everything starts when a transmitter device sends a unicast frame to a device. The receiver device uses a cyclic redundancy check, aka 'CRC,' to confirm the integrity of the data packet reception. If the CRC passes, it means the data packet has not been corrupted during transmission.

The receiver device will send an 802.11 acknowledgement 'ACK' frame back to the transmitter device, as a way to verify the data packet delivery. If during the transmission of the information, a collision happens or a part of the unicast frame is corrupted, the CRC will fail. Thus the receiver device won't be sending an ACK frame to the transmitter device.

In turn, the transmitter device will transmit the frames again, causing retransmission. Retransmissions have a high impact on WiFi networks as it creates extra MAC layer overhead, and consumes additional airtime in the half-duplex medium.

Layer 2 retransmissions have a negative effect, for instance, the throughput goes down, and latency goes up, impacting voice and video mostly. So, an increase in latency will result in echo problems, and high variations of Jitter will bring as a consequence disjointed audio.

The reasons for layer 2 retransmissions can be quite a few. For instance, a radio frequency interference paired with low Signal to Noise Ratio (SNR) due to a bad WiFi design, both happening at layer 1. Furthermore, there's the possibility of adjacent cell interference and a hidden node that can also cause higher percentages of layer 2 retries.

Layer 2 - Continuation

Roaming

Another common problem in layer 2. Sometimes roaming problems occur due to drivers' issues on the client device side, and sticky devices due to bad WiFi design. Usually, roaming improves for those client devices that support 802.11K protocols.

Furthermore, roaming has a correspondence with WLAN security. When client devices roam from one AP to another, they always need to go through an authentication process with the new AP. When AP's act independently, establishing an authentication takes place every time the client device roams.

For instance, an end user's smartphone is connected to the airport's WiFi – where dozens of AP's coexist in the same network. If the end-user is on the move, without the inclusion of standards 802.11r/k, the smartphone disconnects from the existing AP before establishing a connection with the new one.

As a result, the end-user experiences WiFi disconnection and latency while reconnecting to a new access point. It translates into dropped WiFi-based calls, websites loading slowly, difficulties in uploading images on social networks, and other negative performance.

The Tanaza WiFi cloud platform supports the current fast roaming IEEE 802.11 protocols. The **fast roaming** standards are leveraged when a client device is connected to a secured-password or captive SSID in a wireless network. The standards **allow the client device to roam quickly** from one access point to another in a seamless way. The client devices do not need to re-authenticate to the RADIUS server every time they switch access points.

By installing the **TanazaOS** operating system on access points that do not have roaming within the stock firmware**,** the network administrator can add roaming features following the IEEE 802.11r/k/v standards. Consequently, it enables the fast roaming feature on top of multi-vendor networks of a wide variety of devices. TanazaOS can run on a wide range of access points, from the cheapest to the most performing ones.

Layer 2 - Continuation

Connectivity problems

Like security mechanisms for authentication PSK or 802.11X and association, it is another remarkable problem in layer 2. If you are using a simple static PSK or if you are using a PPSK solution, where everybody has a unique password key - that is assigned to each device and bound the MAC address, the common problem might be related to a passphrase mismatch. The problem can reside in the access point or in the client device - which makes up for most cases. So if the authentication fails, it means someone is handing the wrong passphrase. A monitoring tool here that tells you that can help.

The other potential connectivity problem can lie on the 802.11x, a port-based access control standard, which is the most secure method for wireless security. Still, it does involve a wide range of components, thus having too many different points of failure in consequence.

If its a backend problem, it means a communication problem between the access point and RADIUS server. So if the RADIUS server can't reach the access point, it could be due to a shared mismatch or incorrect IP settings either on the access point or RADIUS server. Another potential problem could be an authentication port mismatch or an error in the LDAP communications between the RADIUS and the LDAP server.

Certificates

If it's not backend issues, then most likely it has to do with certificates. If an SSL negotiation fails, it can be due to certificates problems. Many things can go wrong with 802.11x certificates that trigger this error, like expired certificates, root certificates installed in the wrong place, incorrect clock settings, or a simple mismatch of EAP types.

If it is not a certificate problem, it can be on the supplicant side (credential problems), like a mistyped password, expire password, or user account. Also, it could be that the user does not exist in the LDAP, or there is a confusion in how it was configured by user authentication or machine authentication.

Layer 2 - Continuation

Connectivity problems

Like security mechanisms for authentication PSK or 802.11X and association, it is another remarkable problem in layer 2. If you are using a simple static PSK or if you are using a PPSK solution, where everybody has a unique password key - that is assigned to each device and bound the MAC address, the common problem might be related to a passphrase mismatch. The problem can reside in the access point or in the client device - which makes up for most cases. So if the authentication fails, it means someone is handing the wrong passphrase. A monitoring tool here that tells you that can help.

The other potential connectivity problem can lie on the 802.11x, a port-based access control standard, which is the most secure method for wireless security. Still, it does involve a wide range of components, thus having too many different points of failure in consequence.

If its a backend problem, it means a communication problem between the access point and RADIUS server. So if the RADIUS server can't reach the access point, it could be highly probable is because of a shared secret mismatch or incorrect IP settings either on the access point or RADIUS server. Another potential problem could be an authentication port mismatch or an error in the LDAP communications between the RADIUS and the LDAP server.

Channel utilization

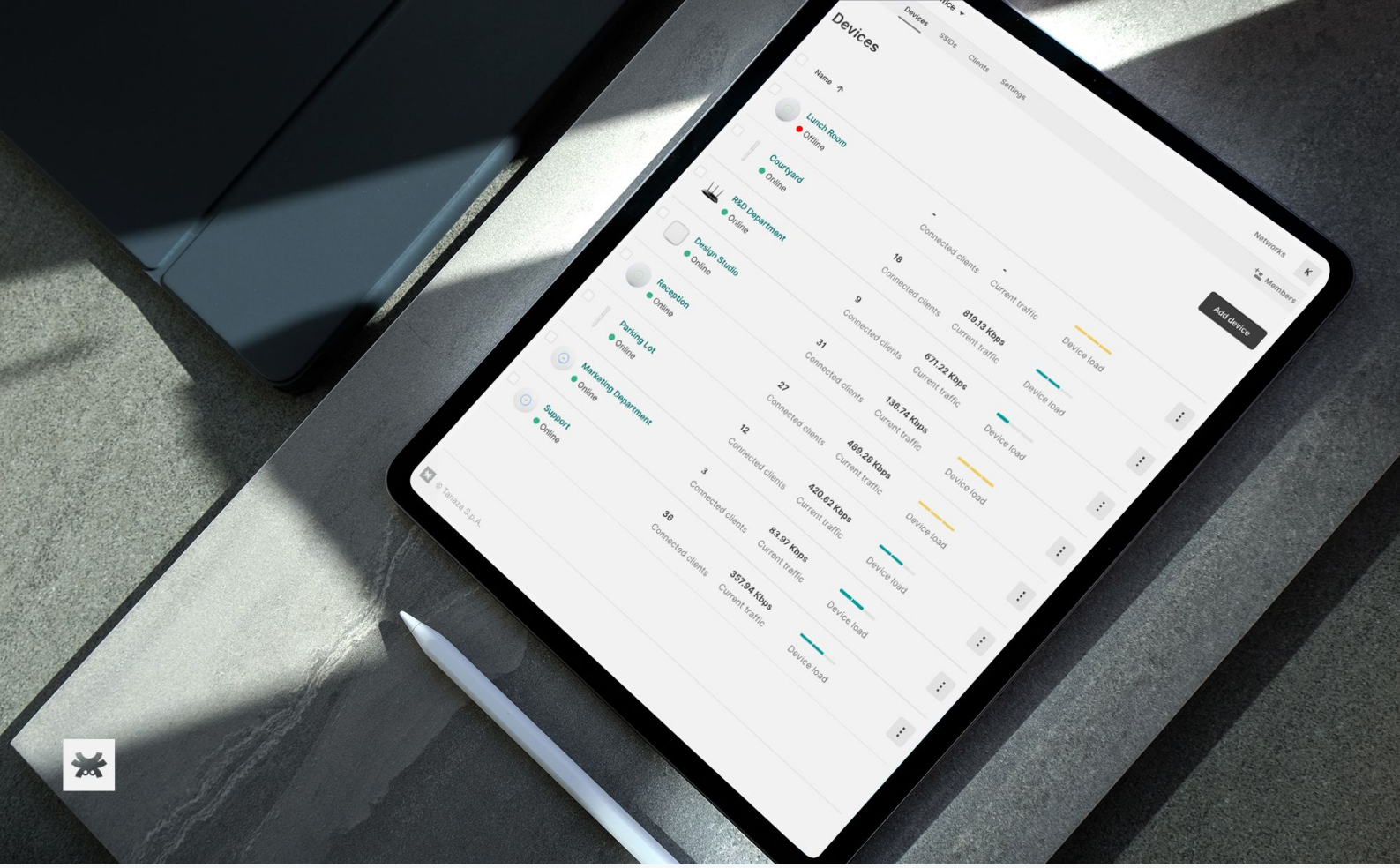
A remarkable statistic to look at when troubleshooting is channel utilization. Here you have some thresholds as guidance:

- 80% of channel utilization impacts all 802.11 data transmissions due to a lot of saturation because of multiple concurrent client devices.
- 50% of channel utilization affects video streaming
- 20% of channel utilization impacts voice traffic.

It's important to always monitor channel utilization, as WiFi networks' performance is highly perceived by end-users. For instance, if a customer complains that the WiFi is slow, then if the channel utilization is over the 80% threshold, then there you have the answer.

Indeed, an overload of concurrent client devices with bandwidth-consuming applications might lead to higher airtime on a channel. Also, when there are too many broadcast SSIDs, limited bandwidth on access points, and an excess of legacy client devices, there's more airtime consumption that, in turn, affects channel utilization.

Rule of Thumb!
If you can prove **the problems are not at layer 1 or 2, it is not a WiFI problem**, which means it is a networking problem, issues with the access points, firewall or application problems. So then you can start troubleshooting at upper-layers of the OSI Model.



Tanaza - The cloud management platform for WiFi access points

Tanaza is a complete cloud platform for IT professionals to manage WiFi networks. Our platform allows MSPs, System Integrators, Network Administrators and ISPs to improve their efficiency levels by managing all WiFi networks, access points, SSIDs and clients from a single platform.

Tanaza simplifies the implementation and configuration of multiple WiFi access points. Users can apply the same configuration to multiple access points simultaneously, each access point added to the network will immediately receive the same configurations as the others.

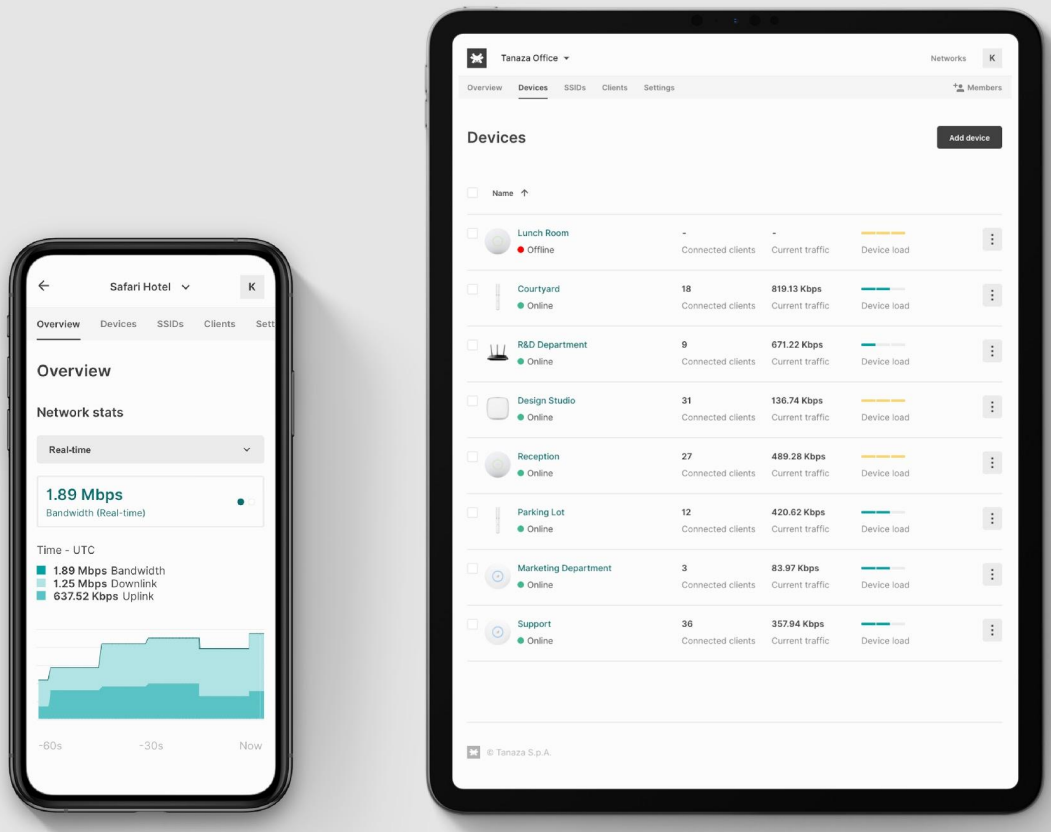
Among the main features of Tanaza:

- Centralized configuration
- Remote monitoring
- Multi-Role Access
- Fast Roaming
- Integrated hotspot with advanced analysis

Manage WiFi access points from the cloud

Manage the settings of hundreds of WiFi access points from a single cloud controller platform. With Tanaza, users can enable SSIDs, configure IP addresses, set radio power and channels, and more from the managed WiFi dashboard. Increase operational efficiency by enabling network-wide configurations and maximize service availability. Users can configure access points without rebooting them or restarting the services.

Tanaza is compatible with the most well-known access point brands on the market, such as Ubiquiti, Amer Networks, TP Link, LigoWave. Alternatively, you can choose from our line of **Tanaza Powered Devices™** : access points with TanazaOS pre-installed, the powerful Tanaza operating system based on Linux.



Experience the power of Tanaza WiFi cloud management in seconds with our free interactive demo.

Try Interactive Demo

tanaza

Discover Tanaza | www.tanaza.com