GRANDSTREAM

CONNECTING THE WORLD

23 Must-Have WiFi Features

Installing, updating or expanding a WiFi network can seem complicated because of the long list of features available and the always-evolving nature of technology. The point of this guide is to cut through all of that and highlight the most important features you should be looking for in order to build powerful, long-range WiFi networks.

Reading through this guide will not only help you better understand all of these features but it will also help you identify your needs. To make it even simpler, Grandstream's GWN series of WiFi Access Points (APs) and Gigabit Routers support all of the features mentioned in this guide.

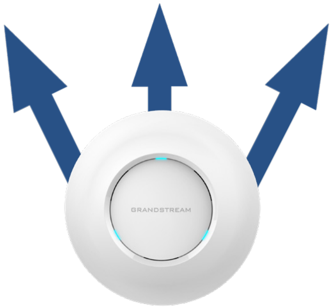
WIFI TECHNOLOGY

1. 802.11ac

Make sure your WiFi access points support the 802.11ac networking standard. It is the latest and most powerful WiFi standard. In general, 802.11 is a set of media access controls (MAC) and physical layer specifications for the creation of wireless local area networks (WLAN). Most 802.11ac APs will also support older standards while giving you a future-proof new AP.

2. Wave 2

Look for APs that support Wave 2, which is the second generation of 802.11ac. It was introduced in 2016 and supports higher bandwidth than Wave 1 (the initial generation of 802.11ac capable APs).

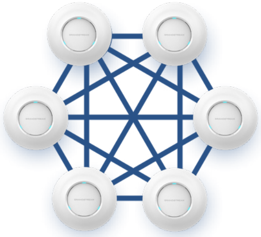


3. Beamforming technology

Beamforming technology allows APs to detect the location of clients and focus their signals towards those clients rather than simply radiating out in all directions. This further enhances network speeds and user support.

4. MU-MIMO

If you have multiple people accessing your network, you will want APs that support MU-MIMO. When WiFi was created 20 years ago, it was built to handle traffic on first-come, first-served basis, which could create network congestion. MU-MIMO, a central component of Wave 2 technology, enables many users to access an AP without causing congestion by allowing all of the antennas on the AP (located internally on the GWN series) to send and receive multiple data streams simultaneously to maximize network speed and client support.



5. MESH Networks

A MESH network is another great way to optimize WiFi speed and efficiency while also providing redundancy in case an AP goes down. A MESH network allows all APs to communicate with each other wirelessly to spread a connection and most efficiently route data to and from clients. Traditionally, WiFI networks rely on APs to communicate through wired connections with other APs and routers, while MESH networks create a wireless connection between all APs, expanding the flow of data on a network. Also, if an AP on a MESH network goes down, other APs can automatically pick up its load.

6. Dual-Band

WiFi has traditionally relied on the 2.4 GHz wireless frequency band. However, as result millions of devices and even other wireless protocols like Bluetooth are all operating on the same band, causing a bottleneck. Most new WiFi APs and clients also support the 5 GHz band, offering a dedicated frequency only for WiFi connections while allowing you to split traffic between two bands to further eliminate congestion.

7. Multiple SSIDs

An SSID is simply a wireless local area network (WLAN). The amount of SSIDs supported by an AP is the amount of different wireless networks it can offer. Our GWN series supports up to 16 SSIDs per device.

8. Load-balancing

Load-balancing is a router feature that distributes network traffic between multiple ISPs (internet service providers) rather than pushing all traffic to one provider, creating a network traffic jam. Aggregating multiple service connections allows a network to handle more users and offer a better overall experience without slowing down each users speed.

NETWORK MANAGEMENT

9 . Embedded Controller

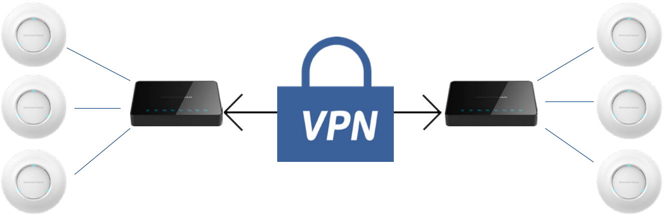
A “controller” is the device or software that sets up and manages a network of APs. Traditionally the controller was separately purchased hardware or software that required a manual setup process. To fix this, we have built an “embedded controller” into our GWN series to allow entire networks of APs to be setup and managed from one central location – the web UI of any GWN series device. It is included at no extra charge and allows you to auto-discover any GWN series APs and auto-provision them, making installation quick and easy while also saving money.

10. Cloud Management Platform

If you want to setup and manage APs in multiple locations or larger networks, then a centralized cloud WiFi management platform like our GWN.Cloud is what you need. These solutions offer a centralized platform that can be accessed from anywhere while managing APs in any location. It provides one centralized interface for an entire deployment while offering real-time data and analytics for all networks, APs and clients. Our GWN.Cloud even makes installation as simple as scanning an APs QR code on our mobile app.

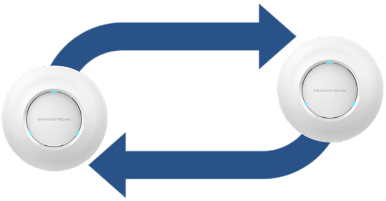
11. Application Prioritization

Quality of Service (QoS) is a feature that allows for the prioritization of certain traffic, applications, ports or MAC addresses within a network. Many APs, including our GWN series, allow users to adjust QoS settings to prioritize certain network traffic or devices so that critical tasks don't compete for bandwidth with less important traffic. For example, ypou can prioritize voice traffic for WiFi voice networks or video traffic for multimedia centers.



12. VPN

A virtual private network (VPN) is a private, protected network accessible through the public Internet. They allow businesses in multiple geographic locations to share networks (and resources) while ensuring security and enabling remote users to access these private shared networks. VPNs can be extended through WiFi APs to offer WiFi access, as long as the VPN is configured with the APs in use.



13 . Network Redundancy

Building redundancy into your WiFi network effectively ensures that it will never go down. Building a MESH network is the best way to create redundancy for your network of APs. This way, if one AP goes down, other APs in the area pick up its load. If you are looking for backend network redundancy, purchasing service plans from multiple ISPs offers a simple redundancy plan, while also allowing your network to utilize beamforming technology.

14. Gigabit

If you want your network to support the fastest possible speeds, make sure your WiFi APs, switches and network routers all offer Gigabit ports to support connections speeds up to 1 GB per second.

WIFI SECURITY

15. Digitally Signed Firmware

Firmware is the backbone of any network as it dictates how APs and routers operate. If someone gets access to your APs firmware, they can completely take over your network. Aside from encrypting firmware files, our GWN series protects firmware by building digital signatures into each layer, which are checked upon reboot or upgrade by the AP/router. This leads to the next feature, critical data lockdown.

16. Critical Data Lockdown

With our GWN series, if the digitally signed firmware is tampered with in any way, the digital signature will fail the verification upon re-boot or firmware upgrade. As a result, the system will block any changes to the firmware and prevent illegally modified firmware from being installed.

17. Random Default Passwords

Every AP has a default password used to access its user interface upon purchase (before you can customize it.) Many manufacturers use the same default passwords or a predictable password pattern, making it easy to hack into these APs at a critical time when the network has not yet been secured. We use a completely different, randomly generated default password for every GWN series device, making them nearly impossible to hack into.

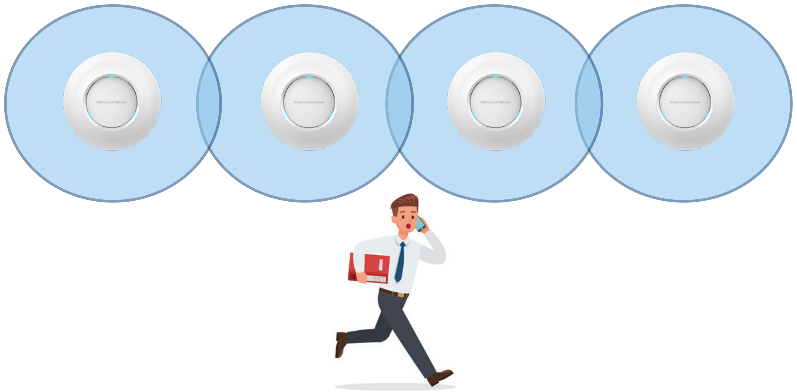
18. Unique Security Certificates

Whenever a connection is made between a WiFi AP and a client, a security certificate is extended to secure the connection. Be careful though, because many AP manufacturers will use the same exact security certificate on all of their APs. This means that if someone is able to hack into one AP, they can hack into every AP that manufacturer makes. Here at Grandstream, we build a different security certificate into every AP to ensure it is nearly impossible to hack into them.

19. Firewall

A firewall is not specifically a WiFi feature but an important networking topic. One of the most common network security measures, a firewall is either hardware or software (now-a-days mostly software) that control all network traffic. It essentially builds a “wall” around the network to prevent unauthorized access and harmful activity while governing all network traffic. The level of protection and control varies by firewall.

CLIENT AND GUEST SUPPORT



20. Roaming

While roaming is a decision made by the client device, the latest generation of WiFi APs offer a variety of features that help WiFi clients make the best possible roaming decisions. There are two features that help this happen and both are supported by our GWN series APs.

20 A. WiFi Voice Enterprise

Specifically built to optimize WiFi voice networks, this utilizes three different protocols (802.11k, 802.11r and 802.11v) to speed up a client's search for APs by providing it with a list of nearby APs and their information. This feature also shortens the authentication period when roaming to a new AP.

20 B. PMK Caching and OKC

For all WiFi connections, Pairwise Master Key (PMK) caching eliminates the need to re-verify authentication when roaming to a new AP in order to decrease authentication time. If Opportunistic Key Caching (OKC) is also enabled, a copy of the PMK information will be extended to all APs on the network to completely eliminate the authentication process while roaming, even if the client has not been connected to an AP previously.

21. Captive Portals

A captive portal is a web landing page that a user must interact with before being granted access to a network. They can be used to require acceptance of terms and services, collect payment, show an advertisement, obtain personal data and even confirm authenticity prior to allowing network access.

INSTALLATION

22. IP66 Certification

If you want to place WiFi APs outside, or anywhere that could be effected by weather, make sure they are IP66-certified, like our GWN7600LR is. IP-66 certification means the devices are waterproof.

PoE

23. PoE/PoE+

Make sure your WiFi APs support PoE or PoE+ so they can receive power and a network connection from one Ethernet cable coming from a PoE switch.