synapse

WIRELESS COEXISTENCE & CONNECTIVITY

- System deployment network diagram
- Key benefits of the SimplySnap solution
- Enablement for ESG Initiatives

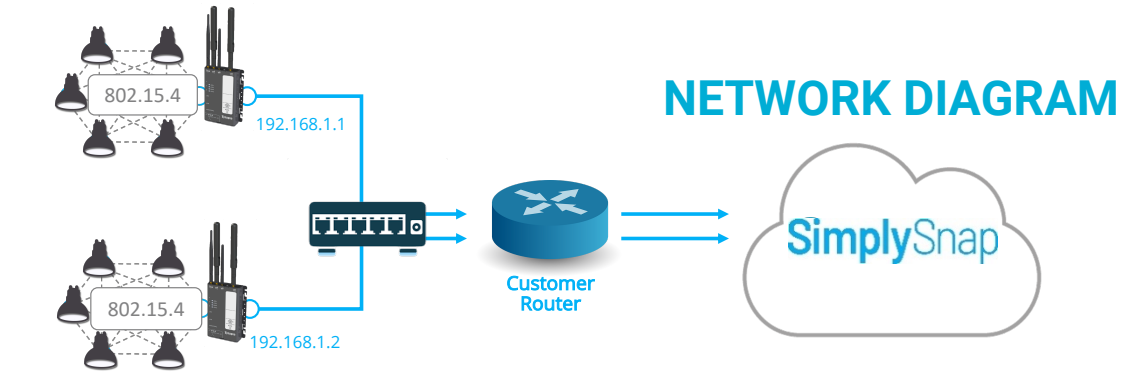
INTRODUCTION

It is hard to imagine a workplace that doesn't incorporate numerous types of wireless connectivity. Wi-Fi networks have become ubiquitous and a necessity to people's lives. In the workplace, companies deploy Wi-Fi networks to facilitate simplified connectivity solutions.

Leveraging a wireless approach that can coexist with established corporate wireless networks, Synapse Wireless' sustainability focus encompasses strategic and targeted solutions to enable organizations to meet their resource management, sustainability and organizational ESG goals. Synapse Wireless delivers actionable insights through the deployment of a wireless and modern cloud architecture integrating existing facility equipment and resources across multiple facilities or domains.

The Synapse SNAP Wireless Solution

Our Synapse SNAP wireless technology incorporates the latest advancements in a secure, wireless architecture that was created to provide high-availability (HA) mitigating typical wireless congestion. Based on the industry standard of the IEEE 802.15.4 wireless protocol, our Synapse SNAP network easily coexists among other deployed IEEE based wireless protocols. A typical Synapse SNAP System deployment is illustrated below.



All communication with the internet is initiated through an outbound connection from the Synapse gateway. No inbound connections are initiated. The outbound ports required to facilitate network connectivity are listed below.

SERVICE	PORT	URI	DESCRIPTION
SSH	TCP 22	tunnel.snap-lighting.com	Provides Synapse Support Team command-line access into customer gateway for remote commissioning and troubleshooting. Can be Enabled/ Disabled by the customer.
NTP	UDP 123	ntp.ubuntu.com	Used to synchronize local clock on gateways.
ConfigSync	TCP 443	couchdb.simplysnapcloud.com	Used to synchronize configuration between Synapse gateways and cloud service.
VPN	UDP 1196	Vpn.simplysnapcloud.com	OpenVPN is used to push configuration to the gateways from the cloud service. Also allows administrator access to the Ui of each SimplySnap gateway from a single web domain.
MQTT	TCP 8883	A25n2uts2ytmw2-ats.iot.us-east-1.amazonaws.com	Used to communicate power and sensor data for SimplySnap connected devices to SimplySnap cloud service.

Benefits of the Synapse SimplySnap Wireless Solution

The key benefits of the Synapse SNAP Wireless Solution include:

- Based on the industry standard of the IEEE 802.15.4 wireless protocol
- Implicit coexistence with other IEEE wireless protocols such as Wi-Fi or Bluetooth networks.
- No modification to your current Wi-Fi or Bluetooth deployments
- No increase in bandwidth or traffic to your existing wireless infrastructure and business networks.
- Reduced time to install leveraging wireless connectivity.
- Self-healing network
- Secure, full 128 Bit- AES encryption

The Synapse SimplySnap Network

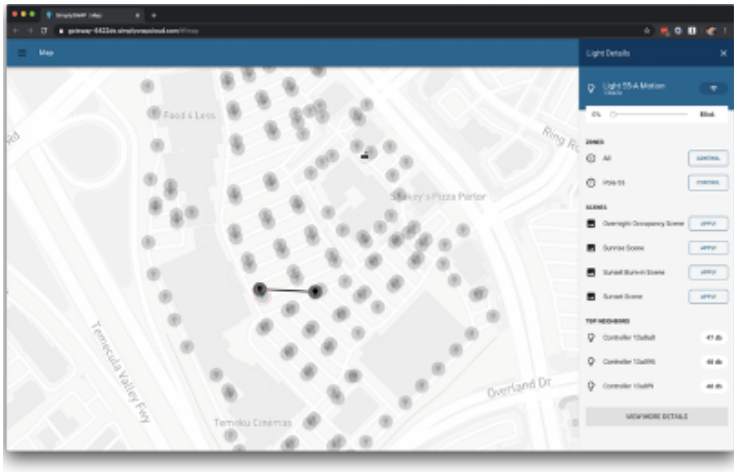
The Synapse SNAP Wireless Solution starts with SNAP nodes. Leveraging the industry standard IEEE 802.15.4 wireless protocol, these nodes form a self-healing mesh network between each other and the SimplySnap Site Controller. With a wireless range of 500 feet line of sight (LoS) for nodes with internal antennas, and up to 1 mile LoS for nodes with external antennas, often a single SNAP mesh network, managed by a single SimplySnap Site Controller, is sufficient to cover a customer's entire facility. Multiple SimplySnap Site Controllers, each with its own SNAP node mesh network, can be combined into a single logical site within SimplySnap Cloud to cover use cases such as:

- Extremely large footprint facilities
- Multi-building campus wide deployment
- Multi-level site garages
- An organic building structure due to numerous facility additions/building add-ons

All communication within the facility between the SNAP nodes and the SimplySNAP Site Controller is secured using 128-bit AES encryption over the SNAP mesh network. Communication from the SimplySNAP Site Controller to Synapse cloud resources are secured using industry standard SSL/TLS protocols.

SimplySnap **Wireless**

- SNAP 802.15.4 @2.4GHz
- Nodes automatically create a full mesh, self-healing network
- Single gateway can manage up to 1,000 devices
- Range up to 1 mile for external and 500 ft. for internal antennas
- SNAP communication is 100% local
- 128-bit AES Encryption



Co-existence of the Synapse SNAP Network with IEEE 802.11 b/g/n (Wi-Fi)

The Synapse SNAP Network is built using the IEEE 802.15.4 wireless protocol for low power, low bandwidth devices. The Synapse SNAP Network utilizes a primary channel that is 2Mhz wide in the 2.4Ghz wireless spectrum. There are sixteen defined non-overlapping channels within the 2.4Ghz wireless spectrum with 5Mhz of total bandwidth associated with each channel. Channel 9, centered at 2.450Ghz, is used as the default network for the Synapse SNAP network, however a different channel maybe configured based on the site wireless characteristics.

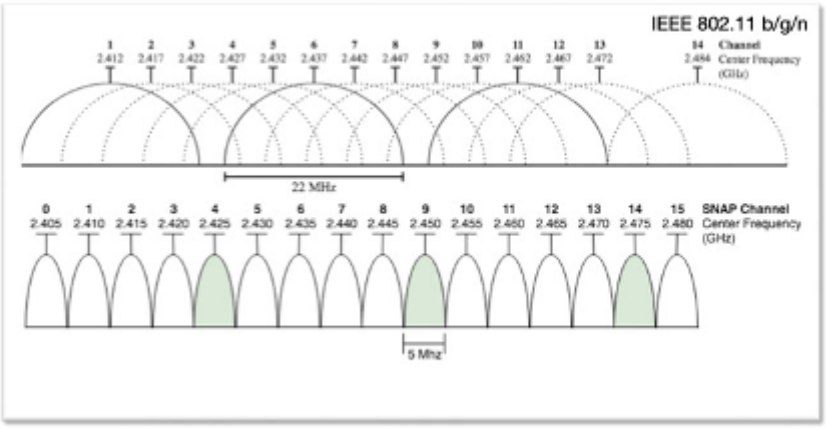
Where can I find more information about the SimplySnap cloud solution?

More information regarding our holistic solution approach can be found on our website at: https://www.synapsewireless.com/

Non-overlapping channels

Regarding Wi-Fi networks, channel 9 was picked as the default channel to minimize any frequency overlap with the standard IEEE 802.11 b/g/n (Wi-Fi) channels of Channel 6 and Channel 11. Each 802.11 b/g/n channel has a bandwidth of 22Mhz. Often in sites with multiple Wi-Fi access points deployed, Wi-Fi channels 1, 6, and 11 are used to minimize interference between adjacent Wi-Fi access points. This is compliant with industry-standard best practices for deploying multi access-point Wi-Fi networks. For this same reason, SNAP Channel 9 is utilized to minimize interference with a deployed Wi-Fi network. The picture below gives a graphical representation of how the different SNAP Channels are defined, along with how SNAP Channel 9 is selected to minimize the interference with Wi-Fi Channel 6 and Wi-Fi Channel 11.

	SNAP Default
Channel	9
Net ID	D110
Encryption	AES-128
CRC	Enabled



Carrier-Sense Multiple Access with Collision Avoidance

Another mechanism that is utilized to facilitate wireless network co-existence is carrier-sense multiple access with collision avoidance (CSMA/CA). Both the Synapse SNAP Network and IEEE 802.11 b/g/n protocols utilize CSMA/CA to minimize over-the-air interference. In this mechanism, a wireless node will attempt to avoid collisions on the wireless bandwidth beginning its transmission of data only after its bandwidth channel is sensed to be "idle". In this way, both protocols attempt to co-exist with each other and nodes only transmit when they think the airwaves are clear.

General co-existence between IEEE 802 Family Protocols

The IEEE Standards Association is an internationally acknowledged and respected group dealing in standards development with voluntary members working in an open and collaborative manner. A significant contribution has been the IEEE 802 standards family, which includes LR-WPANs, Bluetooth and Wi-Fi. For a standard in the IEEE 802 family to be approved, a 'Co-existence Assurance' document must be provided and approved. The co-existence approval process usually involves IEEE members working together to ensure that all 802 wireless standards can co-exist in the same space at the same time (further details on the Co-existence of 802.15.4 with other IEEE standards can be found in Annex E of the IEEE 802.15.4-2003 standard).

How It Works: IEEE 802.15.4 & Direct Sequence Spread Spectrum (DSSS) Transmission

The IEEE 802.15.4 protocol uses direct sequence spread spectrum (DSSS) transmission. DSSS is a spread spectrum modulation technique used for digital signal transmission over airwaves. It was originally developed for military use and employed difficult-to-detect wideband signals to resist jamming attempts. It is also being developed for commercial purposes in local and wireless networks.

In telecommunications, DSSS is primarily used to reduce overall signal interference. The direct-sequence modulation of IEEE 802.15.4 makes the transmitted signal wider in bandwidth (2Mhz) than the information bandwidth (250Khz or 250kbps). After the de-spreading or removal of the direct-sequence modulation in the receiver, the information bandwidth is restored, while the unintentional and intentional interference is substantially reduced.

The stream of information in DSSS is divided into small pieces, each associated with a frequency channel across spectrums. Data signals at transmission points are combined with a higher data rate bit sequence, which divides data based on a spreading ratio. The chipping code in a DSSS is a redundant bit pattern associated with each bit transmitted. This helps to increase the signal's resistance to interference. If any bits are damaged during transmission (due to concurrent wireless transmission of other devices in the same frequency band), the original data can be recovered due to the redundancy of transmission.

The entire process is performed by multiplying a radio frequency carrier and a pseudo-noise (PN) digital signal. The PN code is modulated onto an information signal using several modulation techniques such as quadrature phase-shift keying (QPSK), binary phase-shift keying (BPSK), etc. A doubly-balanced mixer then multiplies the PN modulated information signal and the RF carrier. Thus, the TF signal is replaced with a bandwidth signal that has a spectral equivalent of the noise signal. The demodulation process mixes or multiplies the PN modulated carrier wave with the incoming RF signal. The result produced is a signal with a maximum value when two signals

are correlated. Such a signal is then sent to a BPSK demodulator. Although these signals appear to be noisy in the frequency domain, bandwidth provided by the PN code permits the signal power to drop below the noise threshold without any loss of information.

For more information about DSSS please refer to the following references

- https://www.electronics-notes.com/articles/radio/dsss/what-is-direct-sequence-spread-spectrum.php
- https://www.eetimes.com/tutorial-on-spread-spectrum-technology

WIRELESS Security

Our mesh network uses industry standard AES-128 symmetric encryption over 802.15.4 for RF communication from node-to-node and gateway-to-node. Gateways using SimplySnap Things Services employ WPA-PSK for Wi-Fi based connections and TLS 1.2 over Ethernet. Synapse IoT devices are capable of live Over-the-Air (OTA) updates from the gateway down to the node. This allows Synapse developers to respond to the latest cyber threats to push patches and configuration hardening on-demand.

More information related to our security philosophy, methodologies and current security information can be found on our website: https://www.synapsewireless.com/security/.

Where can I find more information about the SimplySnap solution?

More information regarding our holistic solution approach can be found on our website at: https://www.synapsewireless.com/

6723 Odyssey Drive
Huntsville, AL 35806
(877) 982-7888
synapsewireless.com