Wireless Survey, Analysis, and Deployment Example

Organization - Your City, MO.

Executive Summary

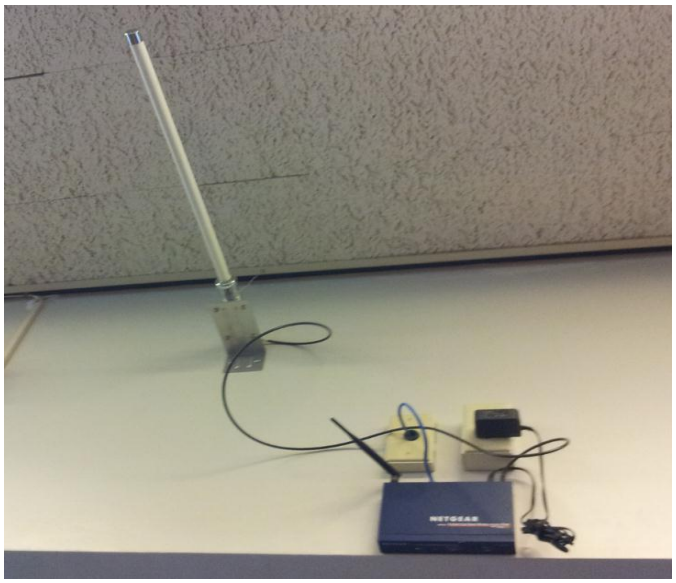
On July 7, 2012, MOREnet performed a wireless survey at the Organization. The purpose of the assessment was to provide analysis of existing and/or future wireless network deployment.

MOREnet staff performed a passive and/or active wireless survey on July 10, 2012 to determine signal propagation and identify sources of interference. Analysis of existing wireless network was also performed. Network infrastructure was also examined to determine support for wireless network.

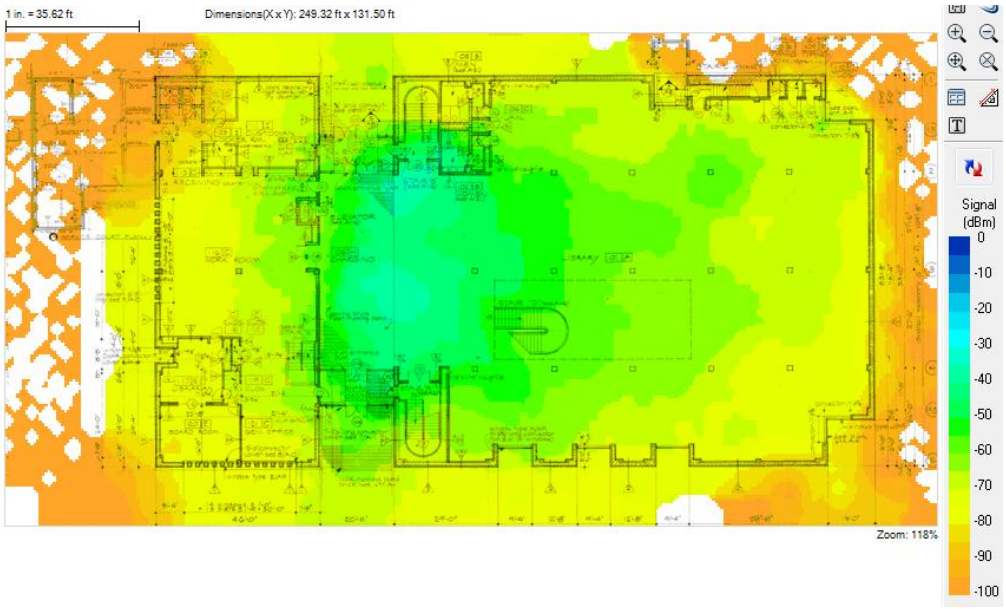
An onsite consultation discussing signal propagation findings, network infrastructure, and wireless solutions formed a recommended wireless deployment and/or improvements. The organization's goals are for the solution and/or improvements here. Public wireless network summary info here deployment. A private wireless network is also planned for staff utilizing wireless summary info deployment.

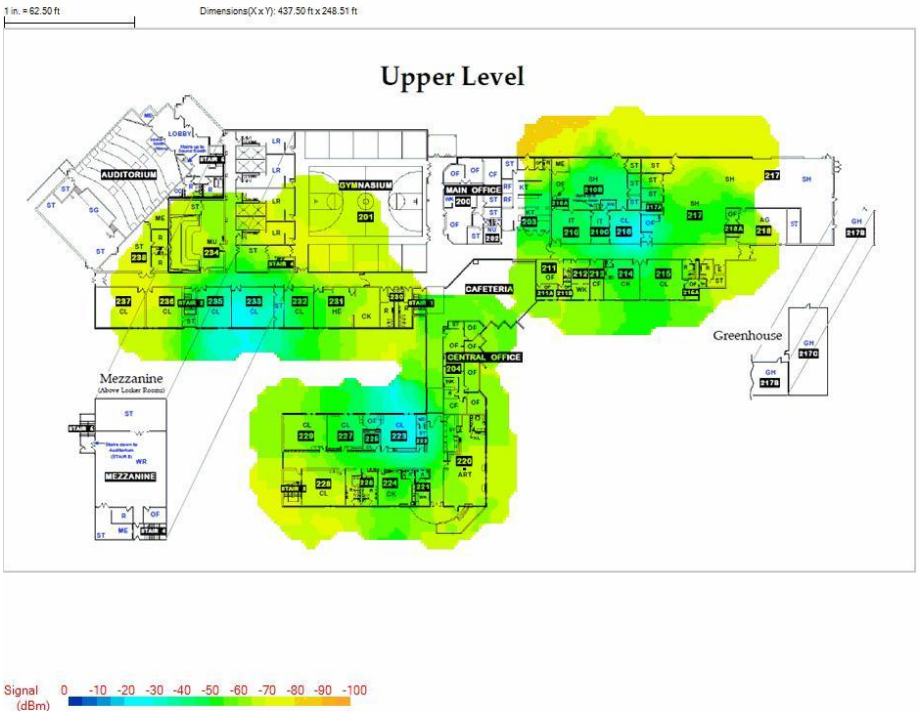
Findings

The organization currently has X wireless network deployed. Staff has an X wireless deployment. Guest access is provided by X wireless deployment. Other wireless deployment observations made here. Several neighbors have wireless networks on various channels but none appear to bleed into the organization at a level of performance or design interference concerns.

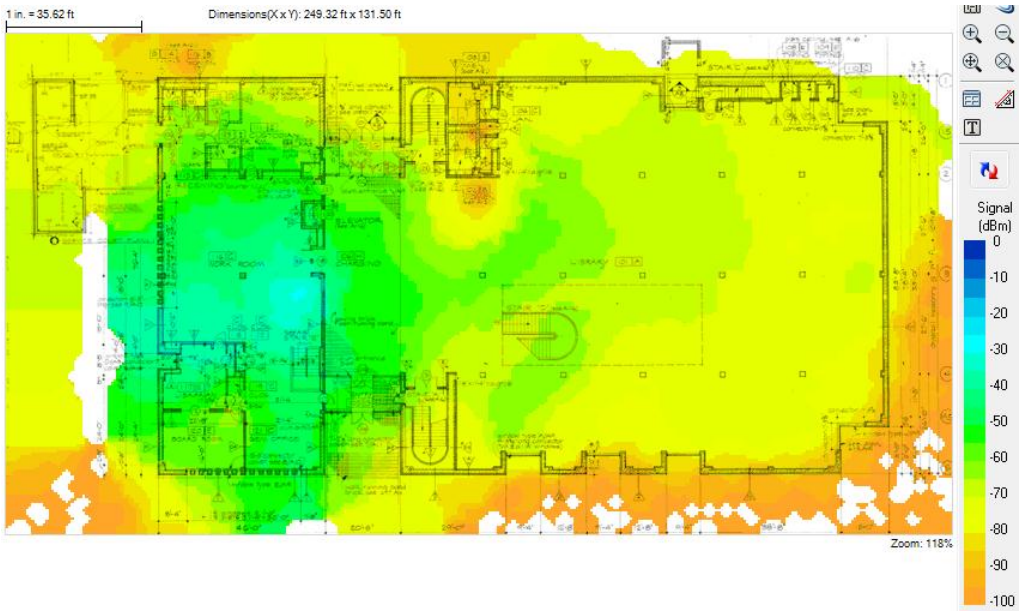


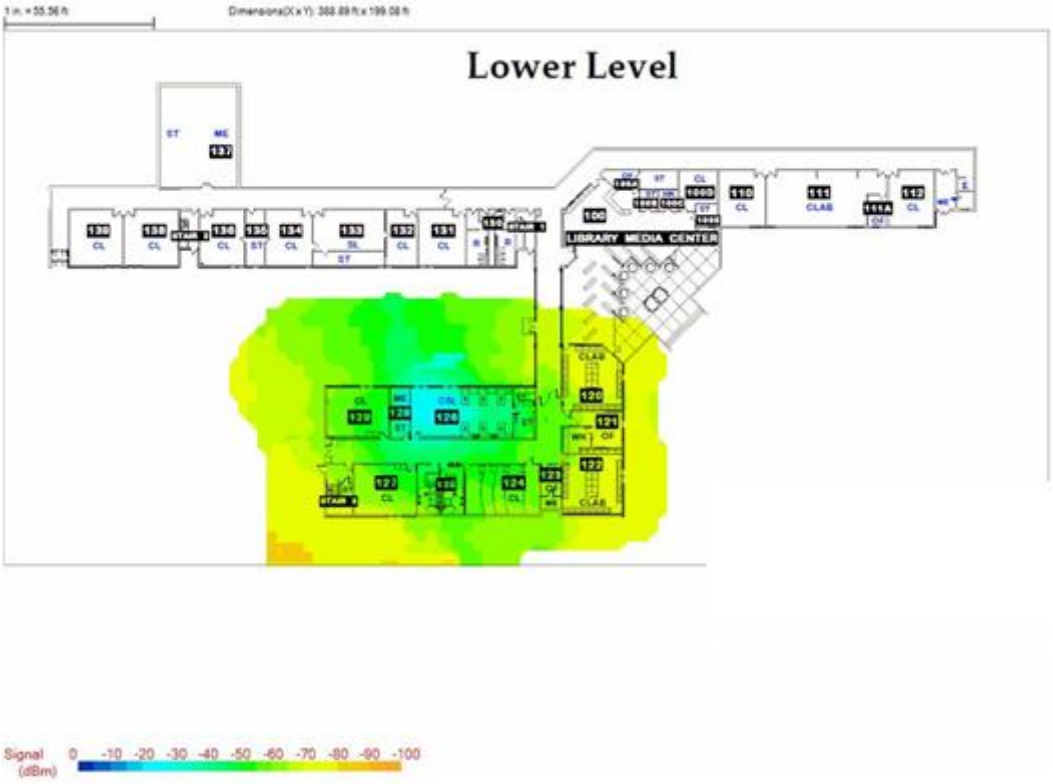
Current Guest Network with SSID “Guest”





Current Staff Network with SSID “Staff”





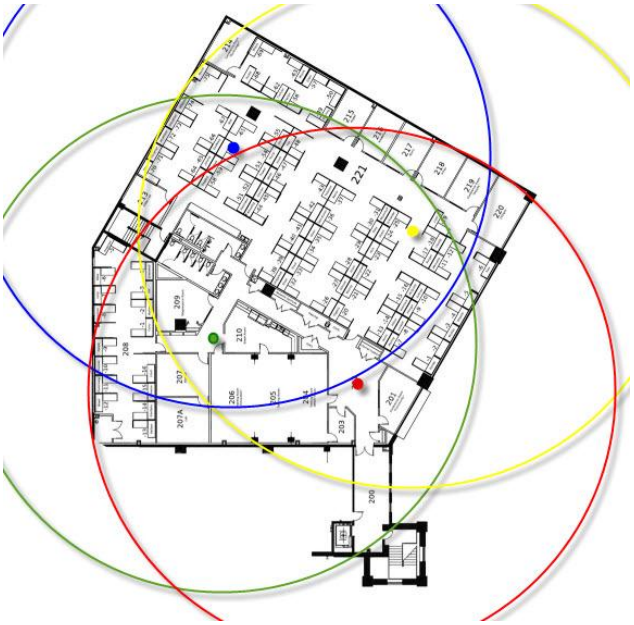
Current Wireless Network Analysis

The following errors were found on the organization's current wireless network.

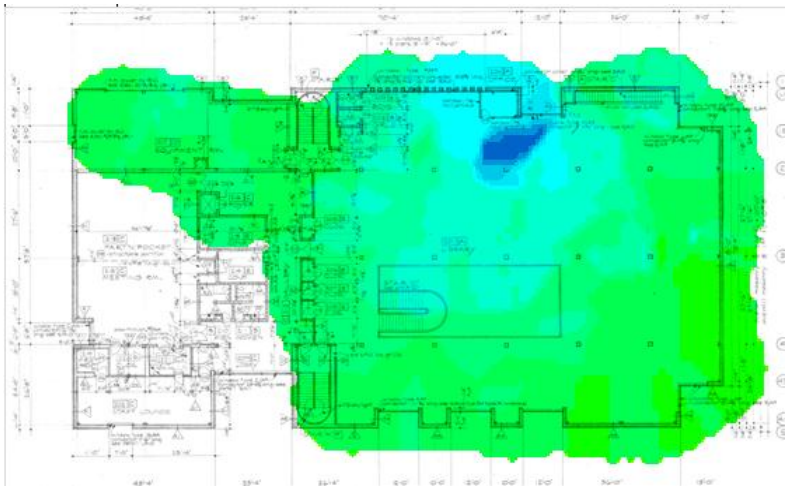
AP Cisco:61:95:C0 (Name: Michael ; SSID : Paradise) 802.11 data link layer frame retry rate (retransmitted frames to total frame ratio) is now 44 %. It has exceeded the alarm threshold of 40 %.
AP Cisco:EB:A1:C0 (Name: Seraphiel ; SSID : Paradise) 802.11 data link layer frame retry rate (retransmitted frames to total frame ratio) is now 85 %. It has exceeded the alarm threshold of 40 %.

The cause of the high frame transmit retry rate may be channel noise, interference, weak signal strength, hidden node syndrome, packet collisions, etc.

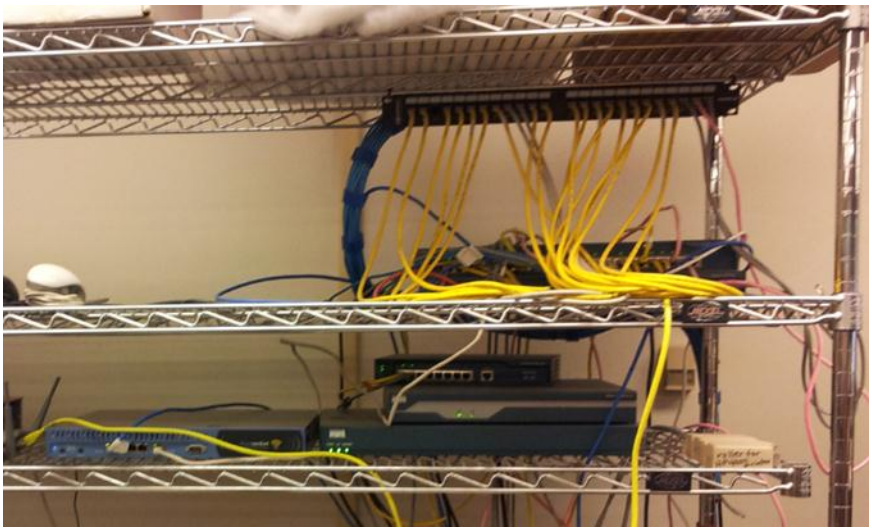
The cause of these errors was determined to be caused by co-channel interference. Access points power are set too high and interfering with each other. This interference is caused by highly overlapping signal coverage cells on the same wireless channel as illustrated below.



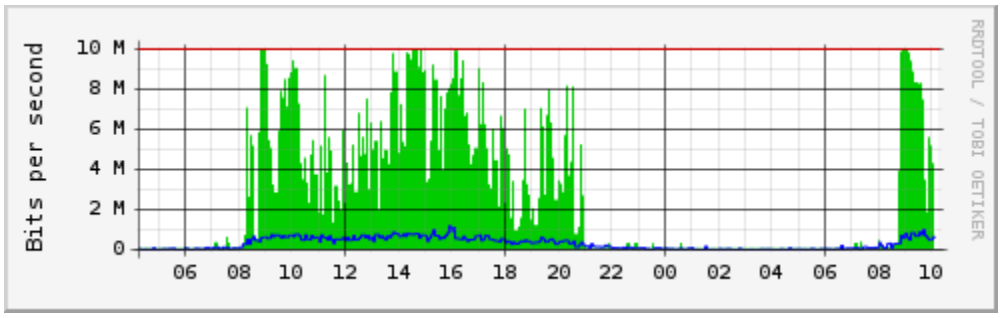
Other sources of interference identified were very occasional use microwave and a cordless phone. The cordless phone appeared to be at determined location. Potential impact discussed here.



The wireless network supporting infrastructure consists of gigabit non-PoE Cisco switches. Static private IP assignment is in use behind ASA firewall. Wireless client IP's are assigned via DHCP. The organization is using MOREnet hosted content filtering. Other wireless network support infrastructure findings inserted here.

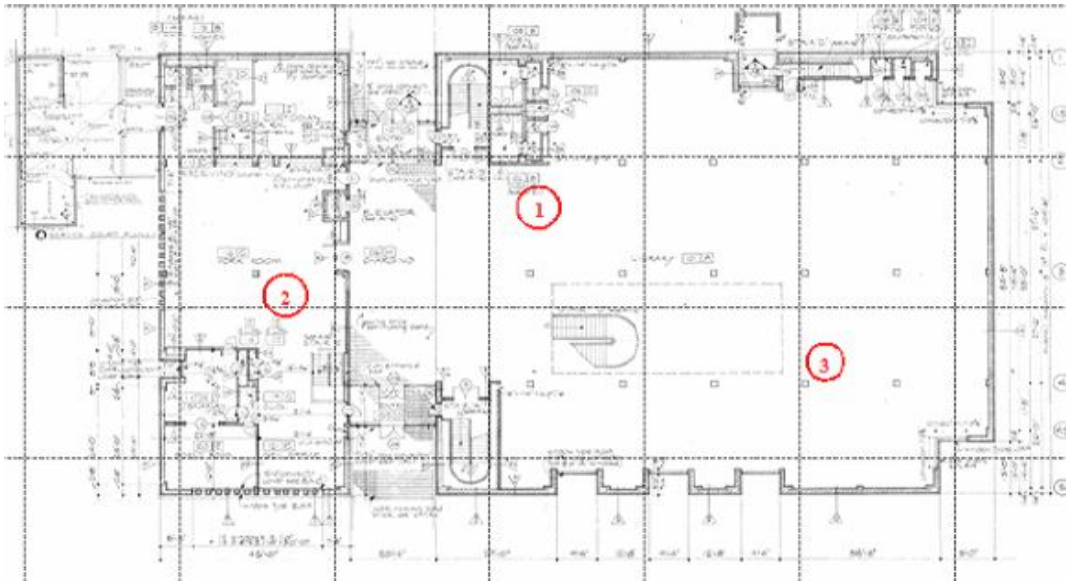


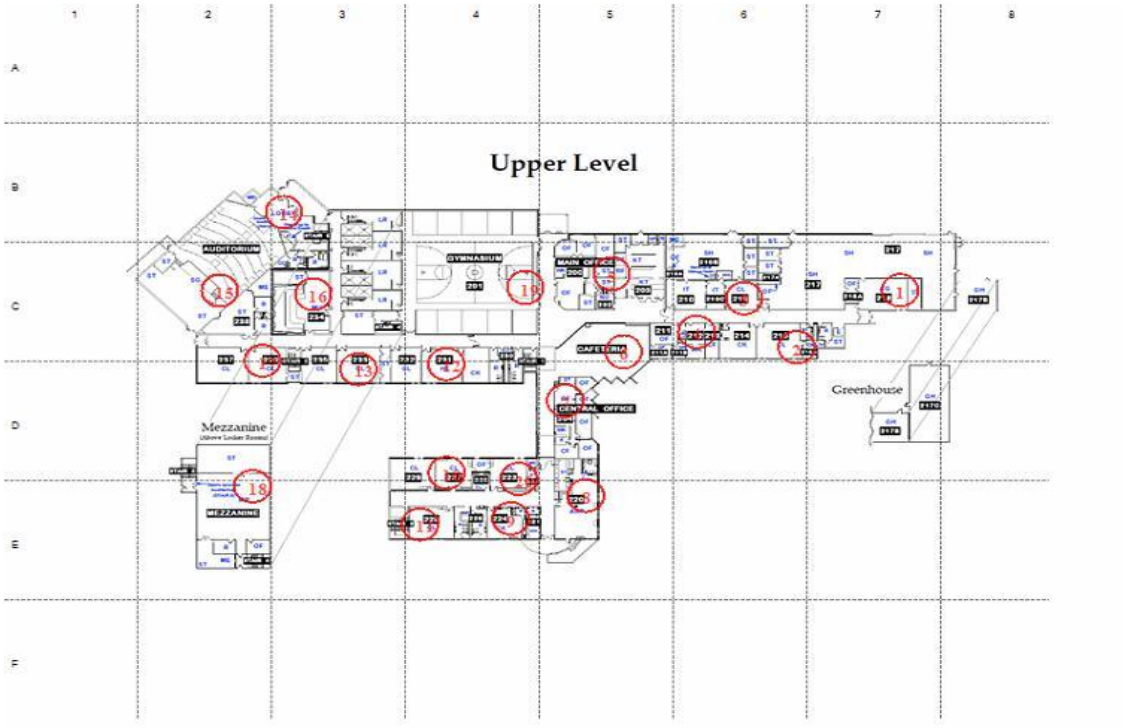
The organization currently has an X internet connection.



Recommendations

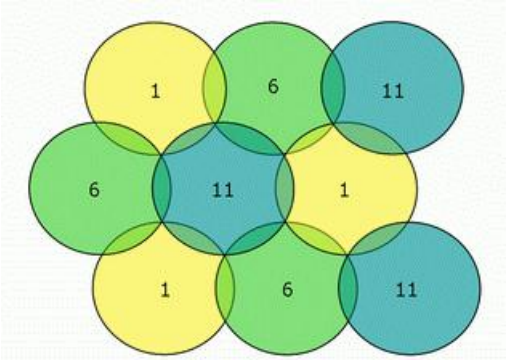
A number of access points cloud hosted Meraki/Aerohive or locally hosted Cisco/Aruba wireless network was quickly identified as recommended solutions. A “V” placement of access points is highly recommended for deployment with one every other classroom for density optimization. Access points should be ceiling mounted at least 10 feet from walls for best performance and to avoid physical disruption. This is a general mounting statement. Some locations like gymnasiums, auditoriums, and outdoor common areas could require wall mounting and/or use of external patch antennas to achieve deployment coverage requirements.

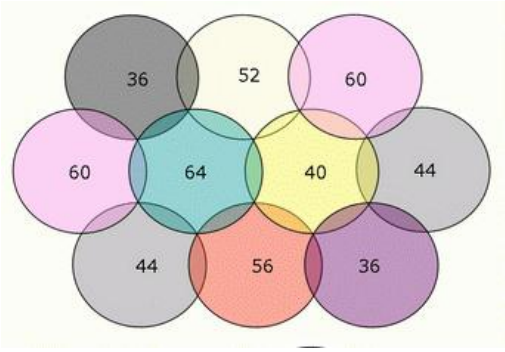




When configuring the type of network each radio band will run, think about the client devices you will be supporting. Legacy device support degrades wireless network performance and features. Ideally, it's best to run the 5 GHz band as an 802.11n only network with 40 MHz channels. IPads and newer notebooks have 5 GHz N support. The 2.4 GHz band is typically set to 802.11g/n, with 20 MHz channels, so there is some legacy support for older devices with G but can still take advantage of some N features such MIMO and beamforming. Most solutions will also let you enable band steering. This provides the ability to force clients that support 5 GHz N to connect on that frequency so 2.4 GHz only devices have less device contention. It also enables the ability to load balance on access points to maximize client density support.

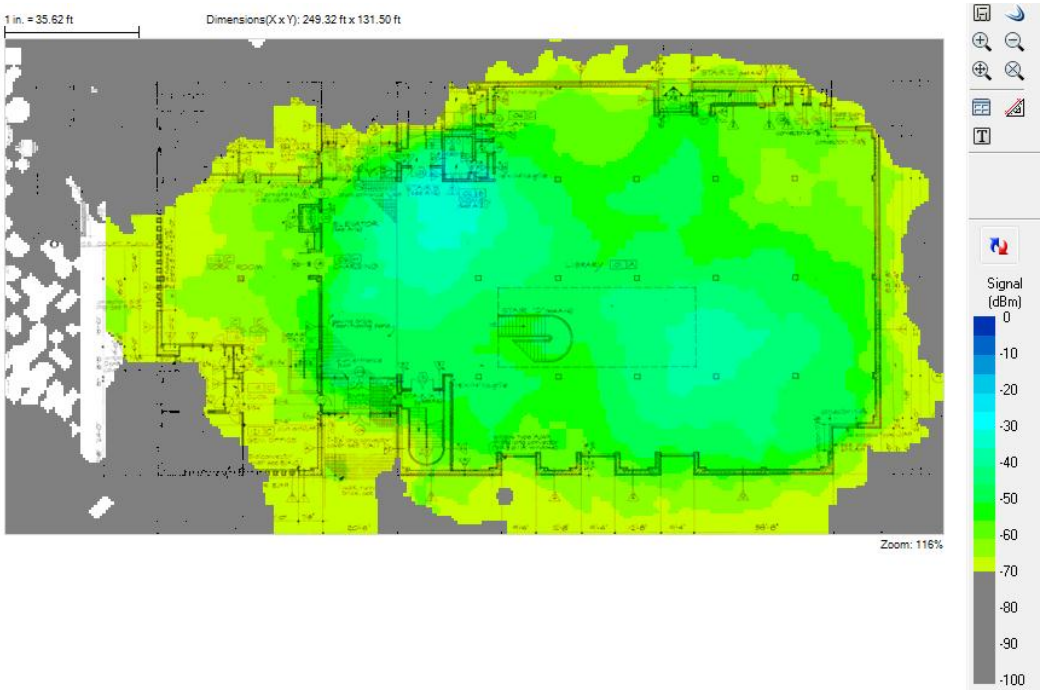
Ensure proper multiple channel reuse. Most vendor controllers will autoconfigure this for you, but the following images can be used as reference if you have to configure manually. Absolutely do not use 40 MHz cannel support on 2.4 GHz.





Microwaves will interfere with the 2.4 GHz network. Don't place access points close to microwaves and try to ensure user connectivity paths do not cross microwave areas

Wirelessly meshed access point could be used in some areas to minimize new network runs. This was tested successfully using Meraki MR16's with the following coverage map.



The organizations current switches are not in need of replacement so it's recommended to use PoE injectors to power the access points. Other infrastructure recommendations here such as PoE switch upgrades and increase power to power the PoE switches.

Security and possible deployment settings were discussed and the following is what the organization will consider for a deployment configuration:

Access Point IP's = Static Private 192.168.1.x range (meshed AP's are automatic, no IP)
Dual band 2.4 and 5 GHz with 5 GHz client band steering to maximize performance
Legacy 802.11b data rates disabled (1/2/5.5/11mb)
2.4 GHz band at 14dB power for small cell high density
5 GHz band at 17dB power for small cell high density similar coverage area as 2.4 GHz

Public Guest Access
SSID = *Guest*
Security = WPA2 personal with pre-shared key (key determined later)
Client IP's = default DHCP with internet access only

Private Staff Access
SSID = *Staff*
Security = WPA2 enterprise utilizing Active Directory
Client IP's = depends on network design needs

Some optional settings such as scheduling, splash page, and traffic shaping were discussed and the organization will address them to fit their needs at a later date.

Wireless users will be filtered the same as entire organization currently is with no need to adjust settings. It is likely the wireless access will increase the organizations usage and they already have or should have a circuit upgrade in process that will address this increase.

The wireless deployment recommendations will generate the following approximate usable signal coverage maps.