Infrastructure Design Guidelines

Revision 4.1

Table of Contents

Introduction

Low-power battery operated Wi-Fi sensors enable the convergence of wireless sensing, voice, data and location tracking applications using a common wireless local area network (WLAN). Wi-Fi sensors bridge traditional telecommunications, data communications and mobile technologies, resulting in ease-of-use and cost savings. A Wi-Fi enabled sensor is a WLAN client device, using the same network technology as wireless laptops and PDAs. A Wi-Fi enabled sensor can be configured and managed remotely through a secure connection. These benefits can result in substantial cost savings over other similar wireless technologies by leveraging the Wi-Fi infrastructure for multiple purposes.

Using a WLAN for sensors is not complex, however, a Wi-Fi sensor does impose different requirements on the network that result in deployment considerations that differ from networks which are optimized for wireless data alone. Voice, data and location tracking applications have different attributes and therefore, different network requirements. In addition, data applications are typically bursty in terms of bandwidth utilization, while a Wi-Fi sensor utilizes a relatively consistent and very small amount of network bandwidth. A critical objective in deploying enterprise Wi-Fi sensing is to maintain similar quality, reliability and functionality as is expected in a wired system. The key issues in deploying Wi-Fi sensors are coverage, capacity, quality of service (QoS) and wireless security.

Healthsense has pioneered the use of Wi-Fi enabled sensors in long-term care, making Healthsense the market leader in technology for aging in place. This document identifies issues and solutions based on Healthsense's extensive experience in enterprise class Wi-Fi sensing and provides recommendations for ensuring that a network environment is adequately optimized for use with Healthsense Wi-Fi sensors.

Equipment Reference

Wireless Access Points:

1. The wireless access point shall be IEEE 802.11g and IEEE 802.3af compliant.
2. The wireless access point will use channels 1, 6 and 11 only in the 2.4GHz band.
3. The wireless access point will use a fixed power level. Level determined by site validation with a Healthsense device.

NOTE: While many different wireless access point manufactures and models are acceptable, there are some restrictions. All unique "extended" features of a WiFi implementation should be tested for compatibility (ie. Meru's Virtual Cell Technology is not compatible with location capabilities). Refer to Network section for specific WLAN configuration guidelines.

Network:

1. Separate VLAN for Healthsense Emergency devices and Monitoring Devices
2. UDP Port 52000 outbound access to Internet
3. Internet Access Policy for VLAN may be limited to these specific Healthsense Data Centers:
    i. 68.65.0.0/20
4. IP subnet assignment is typically a /22 to accommodate sensor growth.
5. Adequate DHCP address pools for large number of device deployments to the HS_WIFI VLAN. This can typically exceed 256 devices.
6. DNS server IP addresses for Healthsense device VLAN should point to these Healthsense DNS servers:
    i. 68.65.4.10
    ii. 68.65.0.10
7. QOS where necessary
8. Automatic failover of Healthsense VLAN to secondary Internet Service Provider.

Switches:

1. Minimum 10/100 POE Ports
2. 802.3af compliant
3. Fiber ports where necessary
4. Managed Layer 2
5. Recommend UPS backup power with capacity for at least 1 hour run time

Router(s)/Firewall(s):

1. Capable of operating in High Availability (HA) mode for redundancy option
2. Recommend monitored failover to secondary Internet service.

Telephony:

1. Landlines (1fb) that are implemented with a standard 10-digit dial pattern.
2. Mobile (cellular) phones are implemented with a standard 10-digit dial pattern.
3. WiFi, VoIP, Digital and keyed phones that are adopted as a “responder” phone need to be accessible through a standard 10-digit DID.

Messaging:

1. Standard carrier based text messaging sent through Healthsense SMTP servers.
2. Standard email messaging sent through Healthsense SMTP servers.

Equipment deployment guidelines

WiFi Access Point Configuration settings:

1. WPA2-PSK SSID: HS_WIFI
    i. (pass key supplied by Healthsense) with CCMP-AES Ciphers for both Multicast and Unicast), No Key Rotation
2. SSID should be hidden (not broadcasted)
3. Unique AP MAC addresses must be beaconed for proper location tracking (No virtual cell can be in use)
4. Client association data activity timeout (client data idle timeout) of at least 20 minutes
5. Multi-data rate capable (down to 1Mbps must be supported)
6. Access points should be configured to only use channels 1, 6, 11

Emergency Signaling and RSSI:

1. Minimum Signal Strength of -50dBm as measured by Cisco Aironet 802.11a/b/g wireless adapter(AIR-CB21AG-A-K9), or equivalent, with access points at 50mW transmit power
2. Communication with at least 1 additional access point at -60dBm for redundancy

Coverage Expectations:

1. Minimum 1 AP reading greater than -50 dBm. For redundancy at least 1 additional AP(s) at -60dBm. Reference as measured by Cisco Aironet 802.11a/b/g wireless adapter(AIR-CB21AG-A-K9), or equivalent, with access points at 50mW transmit power
2. Dynamic power settings must be disabled
3. Avoid placing access points in a row – prefer some Aps to be located near outer edges of structure
4. Stagger placement of access points between floors (avoid floor to floor symmetry)
5. Give priority to achieving signal strength requirements and minimization of co-channel interference when finalizing access point placement

Note: Consult access point manufacturer's specifications for antenna pattern – orient access point (or antennas) to minimize transmission thru floor for best results.

Support Infrastructure:

1. Main Distribution Frame (MDF) equipped with router, PoE Switches, and Backup Power Supplies. Intermediate Distribution Frame (IDF) with edge POE switches where appropriate.
2. Redundancy configuration option for all data equipment – define design and cost considerations for reduced functional operation for different points of failure
3. PoE switches not to be daisy chained (direct connection, “Home Runs” from core closet to switches servicing APs required)
4. Fiber to be used in runs greater than 300 feet between switches

WLAN Manufacturer Specific Requirements:

1. Meru installations must have Virtual Cell disabled if using our location tracking feature,
2. Cisco WLC installations:
    i. 5508 and newer controllers are supported
    ii. Firmware versions 7.4.121 and later are supported
    iii. HS_WIFI WLAN specific settings:
        a. Radio Policy – 802.11b/g only
        b. Quality of Service (QoS) - Platinum
        c. Client Exclusion - Disabled
        d. Client user idle timeout – 3600 seconds
    iv. Global User Idle Timeout at max (100000 seconds)
    v. EAP-Broadcast Key Interval at max (86400 seconds)
    vi. Fixed transmit power, level based on survey results