

Welch Allyn Acuity Network installation

Best practices

WelchAllyn[®]

Advancing Frontline Care™

© 2014 Welch Allyn. All rights are reserved. To support the intended use of the product described in this publication, the purchaser of the product is permitted to copy this publication, for internal distribution only, from the media provided by Welch Allyn. No other use, reproduction, or distribution of this publication, or any part of it, is permitted without written permission from Welch Allyn.

Welch Allyn assumes no responsibility for any injury to anyone, or for any illegal or improper use of the product, that may result from failure to use this product in accordance with the instructions, cautions, warnings, or statement of intended use published in this manual.

For patent information, please visit www.welchallyn.com/patents.

For information about any Welch Allyn product, or to contact your nearest Welch Allyn representative, go to <http://www.welchallyn.com/en/about-us/locations.html>.

Manual DIR 80017361 Ver J



Welch Allyn, Inc.
4341 State Street Road
Skaneateles Falls, NY 13153 USA

www.welchallyn.com

Contents

1 - Introduction	1
Welch Allyn Acuity overview	1
2 - Acuity	3
Implementation	3
Best practices	3
LAN/WLAN requirements	4
Aruba LAN/WLAN requirements	5
Cisco LAN/WLAN requirements	7
WLAN Controller requirements	9
Aruba controller requirements	10
Cisco controller requirements	12
Validation	14

1

Introduction

Welch Allyn Acuity overview

Welch Allyn connected workstations, servers and patient monitors utilize standards based communications protocols including, but not limited to, 802.3 for wired Ethernet and 802.11a/b/g for wireless. This guide specifies the requirements and recommendations needed to successfully complete and maintain a Welch Allyn patient monitoring system in your wireless or wired network.

Implementation and maintenance of a stable and usable integrated network is the sole responsibility of the customer.

Although ultimately your responsibility, Welch Allyn recommends that you conduct a hazards analysis per IEC 80001 to determine if any issues exist that should be mitigated to ensure your patients safety.

2

Acuity

Implementation

Welch Allyn has split the best practices into two groupings to bring transparency in making the changes necessary for success. Some items that are included in an individual group may only function correctly if corresponding changes are made in one or both groups. This inter-dependence makes implementation a company-wide undertaking. If the clinical staff manages the Acuity system and is responsible for its use and maintenance, increased communication of the changes made by the IT staff that may impact the Acuity system and the network is recommended.

To ensure the Acuity system operates as intended, the network must meet latency, coverage, jitter, and other network requirements described in this document and the directions for use. Typically, data flows via UDP/TCP from the medical device to an Access Point (AP), through the Health Delivery Organization's (HDO's) layer-3 network to the wireless controller, through HDO's layer-3 network to an Acuity server. A successful site validation is the final step in ensuring the system is ready for implementation.

In all additions and changes to the hospital physical environment or the network environment, verify coverage and proper system operation continue to meet the requirements indicated in this document and the directions for use. Conduct a hazard-analysis per IEC 80001 to determine if issues exist that should be mitigated to ensure patient safety and to continue compliance with recommendations in this document.

While these settings should not pose a risk to any currently installed systems, it is in your best interest to fully review and understand the implications when making these changes. The Welch Allyn support team and local wireless systems engineer are valuable assets throughout this process.

Best practices

Welch Allyn has identified the following required network settings that improve performance of Acuity systems and Welch Allyn patient monitoring devices. The Performance impact column summarizes the network behavior that may be seen if the best practice is not followed.

The settings in these tables require the expertise of an IT Department or consultant with a similar knowledge base. Each of these recommendations has been reviewed by Welch Allyn to insure minimal impact on existing networks. Settings listed in these tables may affect wired and wireless communications and based on testing should not pose a risk to installed security policies.

You are ultimately responsible for the functionality of the network. Review each of these changes and make sure to backup the current settings before making changes.

LAN/WLAN requirements

Each of the following tables reflects a different equipment manufacturer. To skip directly to the table created for the manufacturer of your equipment, click on one of the following links:

- [“Aruba LAN/WLAN requirements”](#) on page 5
- [“Cisco LAN/WLAN requirements”](#) on page 7

Aruba LAN/WLAN requirements

Best practice	Affected types	Without best practice
Bandwidth ¹ 7% Proportional Bandwidth allocation for APs and Welch Allyn virtual APs/Packet-Shaping.	Wireless	Increased probability of dropped patient data packets on busy wireless networks.
Certificates For out of box operation use Welch Allyn certificates and RADIUS Servers.	Wired, wireless	Welch Allyn will be unable to debug system issues such as monitors unable to connect to Acuity. Hospital is responsible for debugging connectivity issues at installation and throughout system life.
Critical IT support On a Shared or Customer Installed network, the customer shall provide 24/7, mission-critical support for their network	Wired, wireless	Possible extended downtime if network support cannot be reached.
Data rates • a band -- 6Mbps required	Wireless	Vital signs monitors will not connect.
Interference Signal to Noise Ratio (SNR) ≥ 15 dB	Wireless	High noise level causes dropped packets.
Jitter Packet-to-Packet jitter shall be ≤ 400 ms.	Wired, wireless	Dropped packets, data loss and dropped connections.
Labeling Welch Allyn VLAN ports should be clearly marked on the physical switches.	Wired, wireless	Harder to debug system issues. Mixing of IT and patient data could result in loss of data due to broadcast storms.
Network latency Round-trip peak network latency between Acuity Central station and its patient monitor ≤ 800 ms.	Wired, wireless	Dropped packets and data loss.
Packet transport Packets should be passed through switches and routers in cut-through mode, or hardware based switching, not store-and-forward-only mode (applicable to older switches/hubs).	Wired	Dropped packets and data loss.
Power redundancy All network equipment used for patient monitoring shall have a redundant power supply and emergency power.	Wired, wireless	Data loss and downtime due to power outages.
Priority Welch Allyn data should have priority over other data. Welch Allyn data is configured for 802.11e Access Category Voice.	Wired, wireless	Mixing of IT and patient data priority may result in lost data.
QoS Hardware Quality of Service (QoS) support should be configured to map 802.11e QoS bits to a hard-wired tag.	Wired	Increased probability of dropped patient data packets on busy wireless networks.
RADIUS server When using EAP authentication, the controller must be configured to communicate with low-latency RADIUS servers. Unreliable communication with a RADIUS server, even in the presence of a secondary RADIUS server, seriously impedes performance.	Wired, Wireless	Dropped packets, data loss, and dropped connections.
Redundancy Redundant coverage in patient areas (i.e. patient rooms) where patients are likely to be unattended. Labs and Transport areas require only single coverage but redundant coverage is recommended.	Wireless	Prevents the loss of data due to a single AP failure.
Roaming across subnets Keep the Welch Allyn wireless VLAN/SSID flat (no roaming across subnets).	Wireless	Success for roaming across subnets depends on the hospital's Layer-3 network. Hospital is responsible for validation of proper roaming across subnets.
Rules/Firewall Use separate rules and roles for Welch Allyn patient data and other IT data. Rules and roles should be identified using Welch Allyn specific names.	Wireless	IT changes to the Aruba controller that inadvertently affect Welch Allyn patient monitoring are more likely. Patient data subject to issues on wired network such as broadcast storms. Shorter battery life for patient monitors.
Separate VLAN Keep Welch Allyn patient monitors on their own VLAN and SSID.	Wired, wireless	IT changes to the Aruba controller that inadvertently affect patient monitoring are more likely. Patient data subject to issues on wired network such as broadcast storms. Shorter battery life for patient monitors.

Best practice	Affected types	Without best practice
Signal strength First wireless signal: RSSI Value ≥ -65 dBm for (802.11a APs set to 25mW). Second wireless signal: RSSI Value ≥ -70 dBm for (802.11a APs set to 25mW).	Wireless	Dropped packets and loss of connectivity due to poor wireless coverage.
SNMP read-only access Welch Allyn servers (Acuity systems) shall have SNMP read-only access to Aruba controllers to log performance data and generate alerts.	Wired, wireless	Limited ability to proactively respond to system issues. Debugging by Welch Allyn Remote Technical may not be possible. Extended troubleshooting times.
Spanning Tree Protocol (STP) STP should be turned off for the Welch Allyn specific VLAN/SSID. Use resilient links (spanning port fast) for all wired interfaces connected to continuous monitors, wireless controllers, or Welch Allyn Servers.	Wired, wireless	Dropped connections.
Mismatched connections Connections between gigabit and FastEthernet interfaces should be avoided. If these interfaces are configured, use them for light traffic only, and do not rely on auto-negotiation. Ensure that you configure speed and duplex settings to 100Mbps and Full Duplex.	Wired	Unreliable network connection, severely affected appliances connected through the interface.
Connection speed All Acuity systems must be connected to the network using the same Ethernet speed.	Wired	Dropped packets, data loss.
UDP broadcast forwarding Allow UDP broadcasts on ports 7711-7720 from Welch Allyn VLAN to the Acuity Central station.	Wired	Connections cannot be established.
Wired connection Interconnects between all switches and all Aruba WLAN controllers with gigabit Ethernet.	Wired	With only 100Mbps connections dropped packets and data loss can occur.

1. The 7% bandwidth allocation will support up to 20 connected Welch Allyn patient monitors per AP. If no Welch Allyn patient monitors are associated with the AP the bandwidth is free to be used by other devices.

Cisco LAN/WLAN requirements

Best practice	Affected types	Without best practice
Authentication/Encryption WPA2-PSK- AES Only	Wireless	Other encryption methods not supported. No connectivity.
Data rates • a band -- 6Mbps required	Wireless	Vital signs monitors will not connect.
Interference Signal to Noise Ratio (SNR) ≥ 15 dB	Wireless	High noise level causes dropped packets.
Jitter Packet-to-Packet jitter shall be ≤ 400 ms.	Wired, wireless	Dropped packets, data loss and dropped connections.
Labeling Welch Allyn VLAN ports should be clearly marked on the physical switches.	Wired, wireless	Harder to debug system issues. Mixing of IT and patient data could result in loss of data due to broadcast storms.
Network latency Round-trip peak network latency between Acuity Central station and its patient monitor ≤ 800 ms.	Wired, wireless	Dropped packets and data loss.
Packet transport Packets should be passed through switches and routers in cut-through mode, or hardware based switching, not store-and-forward-only mode. (Applicable to older switches/hubs).	Wired	Dropped packets and data loss.
Power redundancy All network equipment used for patient monitoring shall have a redundant power supply and emergency power.	Wired, wireless	Data loss and downtime due to power outages.
Priority Welch Allyn data should have priority over other data. Welch Allyn data is configured for 802.11e Access Category Voice.	Wired, wireless	Mixing of IT and patient data priority may result in lost data.
QoS Hardware Quality of Service (QoS) support should be configured to map 802.11e QoS bits to a hard-wired tag.	Wired	Increased probability of dropped patient data packets on busy wireless networks.
Redundancy Redundant coverage in patient areas (i.e. patient rooms) where patients are likely to be unattended. Labs and Transport areas require only single coverage but redundant coverage is recommended.	Wireless	Prevents the loss of data due to a single AP failure.
Roaming across subnets Keep the Welch Allyn wireless VLAN/SSID flat (no roaming across subnets).	Wireless	Success for roaming across subnets depends on the hospital's Layer-3 network. Hospital is responsible for validation of proper roaming across subnets.
Rules/Firewall Use separate rules and roles for Welch Allyn patient data and other IT data. Rules and roles should be identified using Welch Allyn specific names.	Wireless	IT changes to the Cisco controller that inadvertently affect patient monitoring are more likely. Patient data subject to issues on wired network such as broadcast storms. Shorter battery life for patient monitors.
Separate VLAN Keep Welch Allyn patient monitors on their own WLAN, SSID, and VLAN.	Wired, wireless	IT changes to the Cisco controller that inadvertently affect patient monitoring are more likely. Patient data subject to issues on wired network such as broadcast storms. Shorter battery life for patient monitors.
Signal strength First wireless signal: RSSI Value ≥ -65 dBm for (802.11a APs set to 25mW). Second wireless signal: RSSI Value ≥ -70 dBm for (802.11a APs set to 25mW).	Wireless	Dropped packets and loss of connectivity due to poor wireless coverage.
Spanning Tree Protocol (STP) STP should be turned off for the Welch Allyn specific VLAN/SSID. Use resilient links (spanning port fast) for all wired interfaces connected to continuous monitors, wireless controllers, or Welch Allyn Servers.	Wired, wireless	Dropped connections.
Mismatched connections Connections between gigabit and FastEthernet interfaces should be avoided. If these interfaces are configured, use them for light traffic only, and do not rely on auto-negotiation. Ensure that you configure speed and duplex settings to 100Mbps and Full Duplex.	Wired	Unreliable network connection, severely affected appliances connected through the interface.

Best practice	Affected types	Without best practice
Connection speed All Acuity systems must be connected to the network using the same Ethernet speed.	Wired	Dropped packets, data loss.
UDP broadcast forwarding Allow UDP broadcasts on ports 7711-7720 from Welch Allyn VLAN to the Acuity Central station.	Wired	Connections cannot be established.
Wired connection Interconnects between all switches and all Cisco WLAN controllers with gigabit Ethernet.	Wired	With only 100Mbps connections dropped packets and data loss can occur.

WLAN Controller requirements

Welch Allyn has identified the following requirements specific to a network and Acuity implementation.

While many of these settings involve changes to the controllers themselves, some may involve the wired infrastructure.

Each of the following tables reflects a different equipment manufacturer. To skip directly to the table created for the manufacturer of your equipment, click on one of the following links:

- [“Aruba controller requirements”](#) on page 10
- [“Cisco controller requirements”](#) on page 12

Aruba controller requirements

Best practice	Affected types	Without best practice
Advanced Radio Management (ARM) settings: <ul style="list-style-type: none"> • Power save aware scan = enabled. • VOIP aware = enabled • Scan interval = 180 seconds¹ 	Wireless	APs perform ARM scanning at the time when PSP clients are scheduled to send data, resulting in lost data.
Authentication/Encryption EAP-TLS, WPA2-PSK	Wireless	Other encryption methods not supported. No connectivity.
Channel advertisement Advertise 802.11h capability (Broadcast SSID).	Wireless	Decreased number of 802.11a channels available. If APs are on channels that require 802.11h capability, they will not be available to patient monitors, resulting in RF coverage holes.
Channel Switch Announcement (CSA) Disable.	Wireless	When CSA is enabled, data loss when changing channels may occur.
Client Match Disable	Wireless	Increased probability of disconnects and roams in busy regions of network.
Controller redundancy Aruba controller hardware should include controller redundancy, either one to one or one to many (1:1 or N:1).	Wireless	Failure of a non-redundant controller would cause the entire system to fail.
Data Keep patient telemetry data and general IT data separated using a Stateful Firewall. Acuity rules, policies, and roles should be separated from rules, policies, and rules used for other IT data.	Wired, wireless	IT changes to the firewall policies that inadvertently affect patient monitoring are more likely. Patient data subject to issues on wired network such as broadcast storms. Shorter battery life for patient monitors.
Fast roaming/multi-association Disabled.	Wireless	Dropped packets during patient monitor movement.
Firmware version Use Welch Allyn-validated versions of the Aruba Operating System: <ul style="list-style-type: none"> • 3.2.0.1-WA1 • 3.3.1.19 • 3.3.2.10 • 3.3.2.18 • 5.0.3.3 • 6.1.2.7 • 6.2.1.2 • 6.3.1.6 	Wireless	Using a non-validated version of firmware may induce data loss.
Supported hardware versions <ul style="list-style-type: none"> • 800 • 2400 • 5000 • 6000 • SC1 • SC2 • 620 • 650 • 3200 • 3400 • 3600 • 7200 • MK3(5000) • MK3(6000) • AP60 • AP61 • AP65 • AP70* • AP92 • AP105 • AP125 • AP135 	Wireless	Using non-validated hardware may cause data loss. *AP70 only validated for versions prior to 5.0.3.3
Opportunistic Key Caching (OKC) Enabled.	Wireless	Dropped packets during patient monitor movement.
Quality of Service (QoS) Wireless/Wired LAN shall support Welch Allyn patient data with AC_VO (Access Category Voice).	Wired, wireless	Increased data loss for patient data.

1. Aruba 6.2 and later: adjustable via CLI only, see `rf armprofile` command.

Best practice	Affected types	Without best practice
<p>Security Use the following ACL for Welch Allyn patient monitors:</p> <ul style="list-style-type: none"> • IP access-list session WelchAllyn_ACL • any host 255.255.255.255 udp 7711 7720 permit queue high tos 56 dot1p-priority 7 • any alias Acuity-servers udp 1001 65535 permit queue high tos 56 dot1p-priority 7 • user alias Acuity-servers any permit disable-scanning • any svc-icmp permit • any svc-dns permit • any svc-dhcp permit • any svc-http permit • any svc-ntp permit • any tcp 5650 permit queue high • any tcp 5680 permit queue high • any tcp 5695 permit queue high 	Wireless	Failure for monitor to establish session with Acuity server, increased data loss for patient data.
<p>SSID Configuration Avoid duplicate SSID on the 802.11a and 802.11b/g radios of an AP.</p>	Wireless	Client devices may roam from the 802.11a radio on an AP to the 802.11b/g radio rapidly, creating loss of data.
<p>SSID/Radio settings</p> <ul style="list-style-type: none"> • Radio Beacon Interval set to =100 msec • DTIM set to 10 • a band Only • Enable short preamble • 6Mbps Data rate mandatory • Forward UDP ports 7711 -7720 • Radio High throughput enabled (disabled) • Interval between Identity Requests = 3 • Quiet Period after Failure Authentication=3 • WPA-key-period 2000 • Disable channel 165 	Wireless	Loss of connection and data, patient monitor will not connect.
<p>User role Assign user role based on the RADIUS server class value. Set the class attribute on the RADIUS server to the string that is the role assigned; Welch Allyn patient monitors.</p>	Wireless	Patient monitors not assigned to a role. Unable to connect to Acuity server.
<p>VoIP traffic Limit VoIP traffic on 802.11a to no more than three open connections per AP.</p>	Wireless	Having more than three connections per AP has the potential to increase patient data loss.
<p>Wireless Multimedia (WMM) Enabled.</p>	Wireless	Patient Monitors will disconnect during movement.
<p>WLAN Optimization Aruba recommends the following:</p> <ul style="list-style-type: none"> • Controller CPU utilization <50% • Radio channel utilization <40% • Number of SSIDs per AP ≤4 • Number of clients per AP ≤30 • Controller memory utilization ≥20Mb • Average RSSI of all clients ≥-67 dBm • AP Received packet error rate ≤50%. 	Hardware, wireless	When network performance is outside recommended parameters, potential loss or corruption of data.

Cisco controller requirements

Best practice	Affected types	Without best practice
<p>Channel advertisement Advertise 802.11h capability (Broadcast SSID).</p>	Wireless	Decreased number of 802.11a channels available. If APs are on channels that require 802.11h capability, they will not be available to patient monitors, resulting in RF coverage holes.
<p>Channel Switch Announcement (CSA) Disable.</p>	Wireless	When CSA is enabled, data loss when changing channels may occur.
<p>Controller General (GUI)</p> <ul style="list-style-type: none"> Broadcast Forwarding = Enabled <p>Interfaces:</p> <ul style="list-style-type: none"> Welch Allyn VLAN Interface <p>DHCP Information</p> <ul style="list-style-type: none"> Primary DHCP Server = Primary Acuity IP address Secondary DHCP Server = Secondary Acuity IP address <p>Advanced</p> <ul style="list-style-type: none"> Spanning Tree = Disabled *DHCP Proxy = Enabled (default) <p>Controller (CLI)</p> <ul style="list-style-type: none"> EAPOL Key timeout: change default 1000 to 3000 by using the following command: config advanced eap eapol-key-timeout 3000 	Wireless	Loss of connection and data.
<p>Data Keep patient telemetry data and general IT data separated using a Stateful Firewall. Acuity rules, policies, and roles should be separated from rules, policies, and rules used for other IT data.</p>	Wired, wireless	IT changes to the firewall policies that inadvertently affect patient monitoring are more likely. Patient data subject to issues on wired network such as broadcast storms. Shorter battery life for patient monitors.
<p>Firmware version Use Welch-Allyn validated versions of the Cisco Operating System:</p> <ul style="list-style-type: none"> 6.0.202.0 7.0.116.0 7.0.220.0 7.2.110.0 7.4.110.0 8.0.100.0 	Wireless	Using non-validated firmware may cause data loss.
<p>Hardware supported</p> <ul style="list-style-type: none"> Controller: 4400 series, WiSM1 and 5500 series, WiSM2 Access Point: AP1230ag, AP1131ag, AP1240ag, AP1142n, 1252n, AP 3502, AP 3702 	Wired, wireless	Using non-validated hardware may cause data loss.
<p>Radio Resource Manager (RRM) Settings Enabled (default)</p> <ul style="list-style-type: none"> Customers should ensure AP transmit power and channelization is optimized on VLANs used by Acuity. Cisco recommends enabling RRM. Optimal range should be 11 – 17 dBm. 	Wired, wireless	Increased data loss for patient data.
<p>SSID Configuration Avoid duplicate SSID on the 802.11a and 802.11b/g radios of an AP.</p> <p>Note This is not Cisco-specific. This is a general wireless guideline.</p>	Wireless	Client devices may roam from the 802.11a radio on an AP to the 802.11b/g radio rapidly, creating loss of data.

Best practice	Affected types	Without best practice
<p>SSID/WLAN settings</p> <p>Security:</p> <ul style="list-style-type: none"> Layer 2 Security = WPA+WPA2 <p>WPA+WPA2 Parameters:</p> <ul style="list-style-type: none"> WPA Policy = Disabled WPA2 Policy = Enabled WPA2 Encryption = AES Auth Key Mgmt = PSK <p>Quality of Service (QoS)</p> <ul style="list-style-type: none"> Platinum (voice) <p>Wireless Multimedia (WMM):</p> <ul style="list-style-type: none"> WMM Policy = Required 7920 AP CAC = Disabled 7920 Client CAC = Disabled <p>Advanced:</p> <ul style="list-style-type: none"> Allow AAA Override = Disabled Coverage Hole Detection = Enabled Enable Session Timeout = Disabled Aironet IE = Disabled Diagnostic Channel = Disabled Override Interface ACL <ul style="list-style-type: none"> IPv4 = None IPv6 = None P2P Blocking Action = Disabled Client Exclusion = Disabled Maximum Allowed Clients = 0 Static IP Tunneling = Disabled Wi-Fi Direct Clients Policy = Disabled Maximum Allowed Clients per AP Radio = 200 Passive Client = Disabled Client Profiling = Disabled Media Session Snooping = Disabled <p>Off Channel Scanning Defer:</p> <ul style="list-style-type: none"> Scan Defer Priority = Enable only 6 and 7 Scan Defer Time (msecs) = 2000 <p>DHCP:</p> <ul style="list-style-type: none"> DHCP Server (Override) = Disabled DHCP Addr. Assignment (Required) = Disabled <p>Management Frame Protection (MFP) = Disabled</p> <p>DTIM Period (in beacon intervals):</p> <ul style="list-style-type: none"> 802.11a/n (1-255) = 10 NAC = Disabled <p>Load Balancing and Band Select:</p> <ul style="list-style-type: none"> Client Load Balancing = Disabled Client Band Select = Disabled 	Wireless	Loss of connection and data.
<p>VoIP traffic Limit VoIP traffic on 802.11a to no more than three open connections per AP.</p>	Wireless	Having more than three connections per AP has the potential to increase patient data loss.

Best practice	Affected types	Without best practice
WLAN Optimization Cisco recommends the following: <ul style="list-style-type: none"> • Controller CPU utilization <50% • Radio channel utilization <33% • Number of clients per AP ≤ 25 • Controller memory utilization <70% • Average RSSI of all clients ≥ -67 dBm • AP Received packet error rate <10%. 	Hardware, wireless	When network performance is outside recommended parameters, potential loss or corruption of data.

Validation

The validation process begins immediately following the Acuity System installation. Many of the criteria used to ascertain the stability and usability of the installed system have been covered previously in this document. Testing of these criteria involve the use of a laptop utilizing AirMagnet Surveyor Pro and an 802.11a wireless card. The basic testing requirements are listed in the table below. This testing is standard across all installed 802.11a systems installed by Welch Allyn.

Criterion	Measures	Requirement
Device connectivity	A patient monitor needs to be attached to the system during signal testing to ensure dropout does not occur in edge conditions.	The patient monitor should remain connected without any extended gaps of greater than 4 seconds and should not completely disconnect from the network at any time during the test.
First signal strength	The received signal strength of the nearest AP	RSSI ≥ -65 dBm
Network up-time	Amount of time the network transporting patient data is available during any 24 hour period	Up-time $\geq 99.9\%$ over a 24 hour period
Packet latency	Round-trip peak network latency between Acuity Central station and its patient monitors	Latency should be ≤ 800 ms
Packet-to-packet jitter	Jitter times between packets	Packet-to-Packet ≤ 400 ms
Second signal strength	The received signal strength of the next closest AP	RSSI ≥ -70 dBm
Signal to Noise Ratio (SNR)	The difference between the received signal strength and the detectable noise floor	≥ 15 dB
UDP broadcast	The ability to communicate with the central Acuity monitoring station and patient monitoring devices	UDP Broadcasts between ports 7711-7720 should be in pass-through mode rather than store-and-forward mode