Cambium Networks™

High Density Wi-Fi Deployment

WI-FI FOR LARGE MEETING ROOMS, THEATER-STYLE CLASSROOMS, AND OUTDOOR EVENTS

TARGETED AUDIENCE

This paper is targeted towards those who are contemplating the deployment of Cambium Networks cnPilot Wi-Fi in locations where a high density of both clients and APs are required, but not an extreme density as in stadiums and arena. The best examples of this type of deployment are convention halls, large meeting rooms and ballrooms, theater-style classrooms, and some outdoor events. We will cover Wi-Fi design requirements and specific recommended settings. And, while some mention will be made of systems outside of the Wi-Fi equipment, this paper will not attempt to be a complete guide for wiring, routing, or back-end systems such as DNS, DHCP, or web-caching.

OVERVIEW

High density deployments are not concerned with coverage, but instead, capacity. Listed here are the basic steps that you should undertake to maximize capacity; read further through this document to understand the details.

- Determine capacity requirements
- Expected number of client devices and client types
  - Expected applications throughput and latency requirements
- Survey to determine possible mounting locations, cabling and backhaul needs, and identify possible interference concerns
- Gain control of RF environment
- Use narrow beam and sector coverage antennas where appropriate

- Limit the number of SSIDs
- Use 20 MHz wide channels and disable 2.4 GHz radios where necessary
- Reduce the cell size through Minimum BSS and Multicast rates
- Use ACLs to limit unnecessary traffic
- Use VLAN Pooling, unicast DHCP, and Proxy ARP to limit broadcasts
- Enable load balancing, band steering, air time fairness, and client isolation

WHAT IS A HIGH DENSITY WI-FI DEPLOYMENT?

For the purposes of this document, a high density Wi-Fi deployment does not extend to the extremes that a stadium or arena does. However, it does cover cases such as train stations and airports, large meeting rooms and ballrooms, theater-style classrooms, and many outdoor events such as festivals, county and state fairs. High Density Wi-Fi Deployments require careful planning for channels, AP configuration, and back-end services. However, they do not go to the extremes needed for placing APs in very close proximity to each other the way that stadiums and arenas do. For this reason, there are more options for AP placement, which we will discuss further.

FIRST STEPS FIRST

Before you can even begin to design your network, you will need to truly understand what connectivity is required and what is possible. What client devices are expected? Smart phones will always be part of the mix, but can be laptops or even tablets, particularly in the case of a theater-style classroom or large meeting rooms. Convention halls will generally involve a mix of client types. In some cases, there will be areas where client density is not as high and for those, smart phones will become the limiting factor on coverage. However, this document will focus on those areas where density and, therefore, capacity is the deciding factor and not coverage.

What applications need to be supported? Is it simple web browsing or will a special multi-cast application be provided to enhance the experience of spectators? If the venue is a horse race track, there will likely be a need to support very low latency applications for betting. How much upload traffic do you expect vs download? A music festival will experience a lot of uploaded video streaming, which will be a strain on the network. POS (Point of Sale) will be a concern for festivals. Multicast applications are being used more and more often in schools. You will need to have a thorough discussion with the venue owners to determine requirements. Doing this will be the basis for determining the number of APs required, and how many clients each AP will support.

USER TYPE	APPLICATIONS	MINIMUM BANDWIDTH	MAX LATENCY TOLERANCE
Guests/attendees	Web access	300 kb/s	Medium
	Email	200 kb/s	High
	Video streaming	384 Kb/s - 1 Mb/s	Medium
Ticketing	Ticket Scanning	200 Kb/s	High
Services	POS	Varies	Varies
Venue Staff	Web access	300 Kb/s	Medium
	Email	200 Kb/s	High
	VoIP	100 Kb/s	Low

TABLE 1: TYPICAL APPLICATION THROUGHPUT AND LATENCY REQUIREMENTS

GAIN CONTROL OF RF ENVIRONMENT

As much as is possible and practical, obtain control over the RF environment. In nearly every high density Wi-Fi deployment there will be multiple uses for a Wi-Fi network. Vendors at a festival or fair will need POS capabilities. Hotel staff use Wi-Fi not just for guest access, but also for staff needs. Universities also have Wi-Fi needs for their faculty and staff. Design the Wi-Fi network to support the specific needs of the user base. If you do not, they will likely deploy their own, causing interference issue for both of you. Sometimes, this is not possible as an organization involved at an event might require specific Wi-Fi deployment needs by contract. Work with them to assign a minimal number of channels for them to use, keeping as many for your own network as possible, but do coordinate with and police this agreement.

WHICH AP MODELS

Outdoor locations will necessitate outdoor rated APs. Certain Indoor locations might also benefit from outdoor rated APs as well. The reason for this is that two models of outdoor APs, the cnPilot e501S and e502S, are equipped with directional, higher gain antennae. A higher gain antenna will provide better signal strength to those clients it serves while also using an antenna pattern that is more focused, allowing it to "hide" better from other APs.

INDOOR APS

cnPilot e600

The cnPilot e600 is a 4x4:4 802.11ac AP. This is the top performing indoor AP Cambium Networks provides. More performance, here, translates to more capacity. A 4x4:4 AP can provide more throughput to a single client, but it can also make better use out of MU-MIMO, allowing for downlink traffic to up to 4 devices simultaneously, increasing capacity significantly. The e600 utilizes an omni-directional antenna but aided by the power of MU-MIMO.

OUTDOOR APS

cnPilot e500

The cnPilot e500 is a 2x2:2 802.11ac AP with an omni-directional antenna. It is designed with an IP 67 enclosure to operate outdoors, so it can handle the weather and temperature variances that you could expect. This AP will not be the one used most often in this type of venue because of the omni-directional antenna. However, there are locations where it will fit well, areas where crowds are not as likely to be dense and where mounting locations can be obtained readily and the APs can be placed relatively close to those crowds.

cnPilot e501S

The cnPilot e501S is a 2x2:2 802.11ac AP with a 90-120 degree antenna with higher gain than the e500. It is designed with an IP 67 enclosure to operate outdoors. With a directional antenna that provides greater range, this is the AP best suited for most mounting locations in both Convention Hall and Outdoor Music Festival type deployments.

cnPilot e502S

The cnPilot e502S is a 2x2:2 802.11ac AP with a 30 degree antenna with higher gain than the e500. It is designed with an IP 67 enclosure to operate outdoors. With a directional antenna that provides greater range, this is the AP best suited for most mounting locations in Outdoor Music Festival type deployments.

WHERE TO MOUNT APS

The trick is to place APs such that you can obtain as high of a signal strength as possible to the client devices served while also hiding that signal as much as possible from other APs. In order to support a high density of client devices, you will need to deploy more APs than is typical, this means that they will be placed close together. In some cases, such as for outdoor events and in large, open rooms (such as for a convention hall), you will be limited in places where APs can be mounted. This will often lead to situations where APs must be placed close together. For this document, we will use the examples of a theater-style classroom, an outdoor music festival, and a conventional hall.

THEATER-STYLE CLASSROOM

This is an example of high density compounded with a need for high throughput to each client device. However, it is also an example where high density does not necessarily mean a very large number of client devices. A theater-style classroom will be limited to the space enclosed by the room. They tend to range from about 100 up to about 800 seats. Assuming high bandwidth requirements for each client, video streaming and large file transfers, each AP will support fewer client devices than for the other examples.

The cnPilot e600 is the best choice for this type of deployment. The e600 has both advantages and disadvantages in high density deployments. The advantage is increased capacity as explained already. The disadvantage lies in the signal propagation. It is more difficult to place a large number of e600s in close proximity and not have co-channel interference. Fortunately, for a theater-style classroom, the number of APs required is rarely so many that each AP cannot be on its own 5 GHz channel. However, it is still wise to mount APs in locations where the surrounding structures provide some isolation between APs in order to allow for more use of 2.4 GHz. Once a determination is made as to how many APs are required, the next step will be which APs and where to mount them.

Low, Along the Walls

This first mounting location might sound unusual. Mount APs low, along the walls of the classroom, no higher than the seats directly in front of them. This will allow the seats and people in them to absorb some of the signal. APs on opposite sides of the classroom will be better isolated from each other.

On the Ceiling

This mounting location is the most common. While APs along the walls, in the back of the classroom and on the sides, can provide access for much of the room, there will likely be a need for more APs that have a clear LOS to people seated in the middle. If the ceiling has exposed beams or other structures like that, mount APs such that those structures can provide some isolation between other APs on the ceiling.

Behind the stage

Mounting 1 to 3 APs, evenly spaced along the front of the classroom, behind the stage, will ensure coverage and capacity for the speaker, wireless equipment, and for those seated in the front. Mount at least one AP high, perhaps near or on the ceiling, and the others low.

OUTDOOR MUSIC FESTIVAL

A venue such as an outdoor music festival can be somewhat complex. The applications supported will range from Point of Sale, to web-browsing, to streaming video both up and downstream. Mounting locations will also be more complex than an indoor deployment.

To make matters more complicated, it is unlikely that Ethernet or even fiber will be available at all mounting locations. Mesh is a possible solution, but keep in mind that utilizing mesh limits capacity. It is better for each AP to connect back to the core network through its Ethernet port. Where it is not possible, or practical to run Ethernet, via copper or fiber, Cambium does offer both point to multipoint and point to point wireless solutions. Utilizing PMP 450 or ePMP 2000 point to multipoint, you can feed bandwidth to pole and other locations where cnPilot Wi-Fi APs are located without having to trench. This is especially beneficial for outdoor events without permanent structures.

The cnPilot e501S AP will be the most common one used at a venue of this type. It provides greater range and more ability to isolate it from other AP due to the sectoral antenna. Outdoor venues, especially where crowds gather in front of a stage, may not have mounting locations other than around the periphery. Mounting the e501S at a height of between 20 and 30 feet will allow for coverage into the crowd. If no mounting locations can be obtained in the middle of these areas, it is possible to mount one AP at, say 20 feet, and another at 30 feet. Use downtilt to point the lower AP towards the crowd closer to the AP and angle the upper AP farther into the crowd, closer to the middle of it. Doing the same on the opposite side will provide overlapping coverage. Downtilting like this also helps to prevent APs on opposite sides of the area from pointing directly at each other.

If mounting locations can be obtained in the middle, make full use of them. Up to 3 APs can be mounted on a single pole and pointing in 3 different directions. If possible, however, mount each one at different heights. Make good use of downtilt to aim the APs toward the client devices that require coverage.

If coverage is desired in parking lots, the e501S is a good choice. The number of APs here will not need to be as many as in the venue area, as capacity is not a concern. Mounting APs on light poles allows provides height and ensures that there is power available. As before, downtilt the APs.

Coverage for areas such as entrance gates, walkways, and food courts are also good locations for the e501S.

Vendor booths and tents are a good place for the e500 to provide coverage for both Point of Sale and for guest access.

CONVENTION HALL

Convention Halls provide an interesting challenge. Throughput requirements will vary from event to event, so plan for the most demanding ones. Some events provide video streaming, and even interactive applications. Point of Sale will likely need to be supported as well. And, multicast may be a requirement as well. New applications that utilize multicast and smartphones in the audience are being used in place of speakers. Some areas of a convention hall will require higher density planning, such as stages and meeting areas, especially where a key note speaker will present. In other areas, client devices will be more mobile, requiring good roaming support.

Make full use of the crowds to help isolate APs from each other. Convention halls, by their nature, will have tall ceilings. Only mounting on the ceiling will make it difficult to isolate APs enough. As with the theater-style classroom, make use of the crowds and the displays to isolate APs by mounting low along the walls where possible. The e600 is the right choice for these locations.

The ceiling will become the most common location for AP mounting in most convention halls, especially the larger ones. The e501S is a good choice for this location. Use the 120-degree antenna pattern to create rows of coverage by these APs, pointing the APs straight down. Utilize structures on the ceiling to isolate APs from each other as much as possible.

CONFIGURING THE NETWORK

Capacity needs will drive the reason for most of the configuration recommendations listed. However, understanding what applications must be supported is very important as well. For example, if multicast applications will be used, be aware that changes will need to be made to the recommended ACL list.

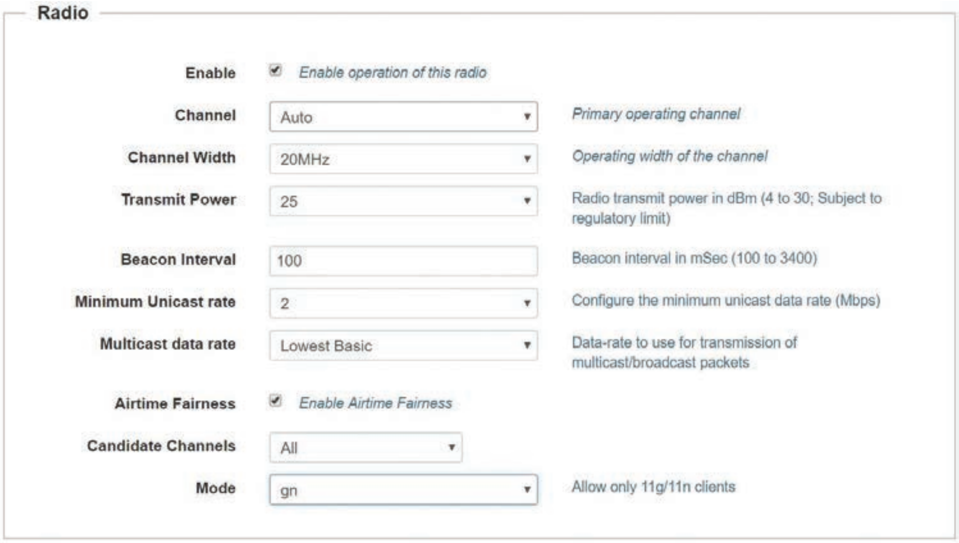
2.4 GHZ RADIO

Both 2.4 GHz and 5 GHz should be used to maximize capacity, although most clients will end up on 5 GHz. However, the 2.4 GHz band is fairly small, limiting the total number of available channels significantly. Depending on the density of APs deployed, it will be necessary to disable a percentage of the 2.4 GHz radios, leaving all 5 GHz radios enabled. For more densely deployed venues, up to ¾ of the 2.4 GHz radios may need to be disabled.

BASIC RADIO SETTINGS

These are the recommended settings for each band.

2.4 GHz Radio



Radio

Enable	☑ *Enable operation of this radio*	
Channel	Auto ▾	*Primary operating channel*
Channel Width	20MHz ▾	*Operating width of the channel*
Transmit Power	25 ▾	Radio transmit power in dBm (4 to 30; Subject to regulatory limit)
Beacon Interval	100	Beacon interval in mSec (100 to 3400)
Minimum Unicast rate	2 ▾	Configure the minimum unicast data rate (Mbps)
Multicast data rate	Lowest Basic ▾	Data-rate to use for transmission of multicast/broadcast packets
Airtime Fairness	☑ *Enable Airtime Fairness*	
Candidate Channels	All ▾	
Mode	gn ▾	Allow only 11g/11n clients

Channel

Enable Auto Channel selection. This will allow the APs to each find the best channel option and to adjust if and when necessary to a new channel. However, it will likely be necessary to disable some of the 2.4 GHz radios on APs that are deployed in particularly dense environments. The 2.4 GHz band is fairly narrow with only a few channels from which to choose. It is important to utilize this band as it will not only add some capacity, but also because legacy devices, such as tickets scanners, often still only support 2.4 GHz.

Channel Width

For 2.4 GHz, 20 MHz channels are the best choice. You will want to use as many different channels as possible, and using a larger channel width will limit that ability.

Minimum Unicast Rate

This setting can vary depending on the deployment. For convention halls and outdoor events, distances to clients can be too far to readily support the highest basic rates. Support for legacy devices such as PoS and ticket scanners may require support of lower PHY rates. Because of that, we recommend a minimum unicast rate of 2 Mbps as the setting to use. However, for theater-style classrooms, choosing either 12 Mbps or 18 Mbps as a better choice as client devices will all be close to the APs.

Multicast Data Rate

This setting can vary depending on the deployment. For convention halls and outdoor events, distances to client devices can be too far to readily support the highest basic rates. Because of that, we recommend “lowest basic” as the setting to use. However, for theater-style classrooms, choosing “highest basic” is a better choice as client devices will all be close to the APs.

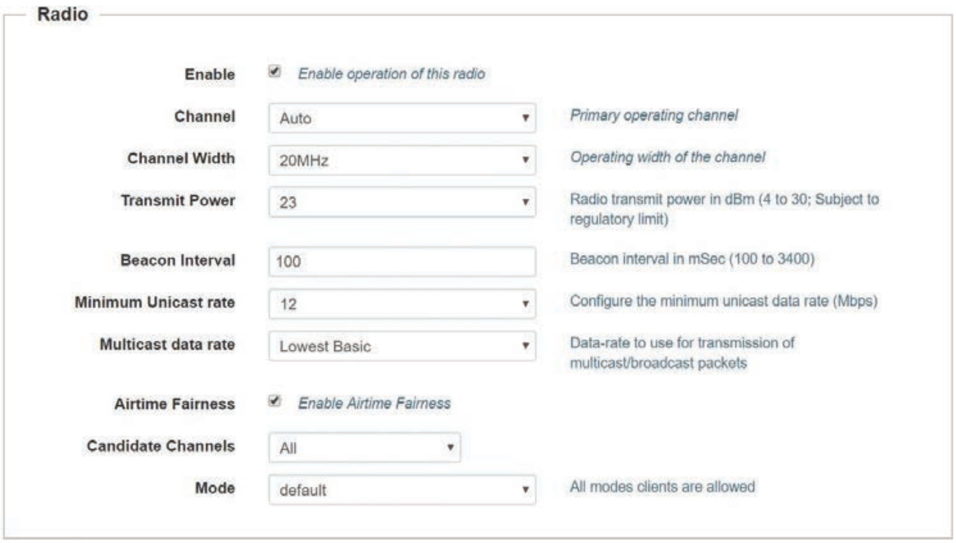
Airtime Fairness

With the improvements to the Wi-Fi standards that 802.11ac brings, Airtime Fairness does not offer as great of a performance improvement as it did previously. Still, there will likely be a few devices operating as 802.11a, b, g, and n. As such, enabling Airtime Fairness will only improve overall performance.

Mode

Be certain to determine if legacy 802.11b clients must be supported. If not, enable mode as “gn.”
If they are, leave this at the default setting.

5 GHZ RADIO



Radio

Enable	☑ Enable operation of this radio	
Channel	Auto	Primary operating channel
Channel Width	20MHz	Operating width of the channel
Transmit Power	23	Radio transmit power in dBm (4 to 30; Subject to regulatory limit)
Beacon Interval	100	Beacon interval in mSec (100 to 3400)
Minimum Unicast rate	12	Configure the minimum unicast data rate (Mbps)
Multicast data rate	Lowest Basic	Data-rate to use for transmission of multicast/broadcast packets
Airtime Fairness	☑ Enable Airtime Fairness	
Candidate Channels	All	
Mode	default	All modes clients are allowed

Channel

Enable Auto Channel selection. This will allow the APs to each find the best channel option and to adjust if and when necessary to a new channel.

Channel Width

Resist the temptation to use large channel widths to obtain greater throughput. The key to capacity when there is a large number of APs in close proximity to each other is to place APs on as many different channels as possible. That means using 20 MHz channels for both 2.4 and 5 GHz radios.

Minimum Unicast Rate

12 Mbps is a good overall choice for this setting in almost any deployment. Even legacy 802.11a devices will support this rate, and at a relatively low SNR. Using lower rates will cause 802.11 management frames to use up more air time, lowering overall capacity. Using a higher rate risks not allowing legacy and distant client devices to connect.

Multicast Data Rate

In the case of convention halls and outdoor events, the best setting is as shown – lowest basic rate. This will allow communications with legacy devices and distant clients. In the case of theater-style classrooms, however, client devices are very unlikely to be legacy ones and will all be close to the APs. As such, a better choice for this setting is “highest basic.”

Airtime Fairness

Enable Airtime Fairness. While more and more clients become 802.11ac capable, there will still be some that connect as 802.11n or even 802.11a or g. Enabling Airtime Fairness will prevent those clients from pulling down the faster clients to their overall throughput limitations.

Candidate Channels

Use as many channels as possible. Some legacy devices may have a problem with DFS channels. If you run into this issue, continue to use all channels, but go to a manual channel plan that disperses DFS channels such that there is enough overlap from non-DFS configured APs to offer coverage for those devices.

Outdoor deployments may run into an issue with DFS channels, such as at an airshow. In this special case, change this setting to non-DFS channels only.

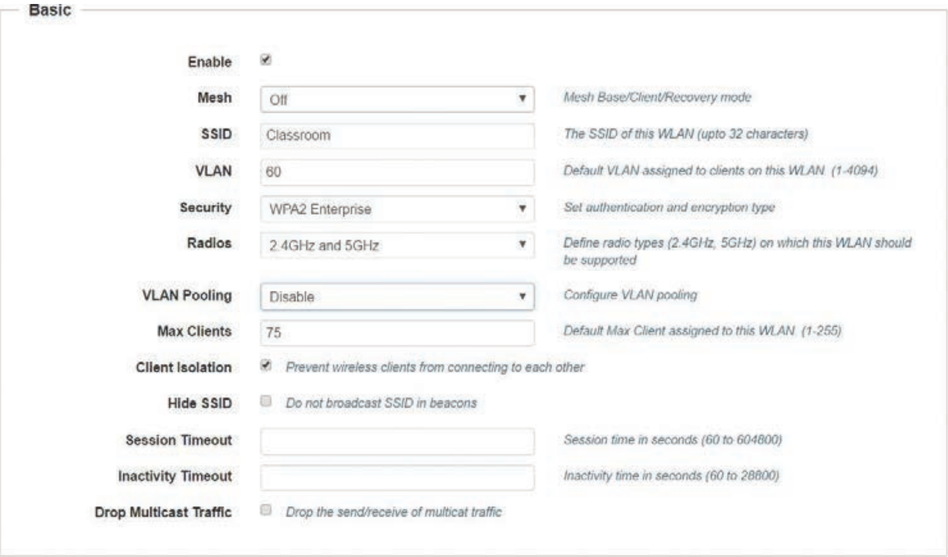
WLAN BASIC SETTINGS

The following are examples of AP configurations for all three of our deployments cases.

Theater-Style Classroom

Mesh

For high density deployments, it is best to avoid mesh where possible. Mesh forces two or more APs to utilize the same channel, and limits the capacity of those APs to that of a single one. In a theater-style classroom, there is no need to utilize mesh.



Basic

Enable	☑	
Mesh	Off ▾	Mesh Base/Client/Recovery mode
SSID	Classroom	The SSID of this WLAN (upto 32 characters)
VLAN	60	Default VLAN assigned to clients on this WLAN (1-4094)
Security	WPA2 Enterprise ▾	Set authentication and encryption type
Radios	2.4GHz and 5GHz ▾	Define radio types (2.4GHz, 5GHz) on which this WLAN should be supported
VLAN Pooling	Disable ▾	Configure VLAN pooling
Max Clients	75	Default Max Client assigned to this WLAN (1-255)
Client Isolation	☑ Prevent wireless clients from connecting to each other	
Hide SSID	□ Do not broadcast SSID in beacons	
Session Timeout		Session time in seconds (60 to 604800)
Inactivity Timeout		Inactivity time in seconds (60 to 28800)
Drop Multicast Traffic	□ Drop the send/receive of multicat traffic	

VLAN

While the use of VLANs is not strictly required, it is a good tool for separating traffic. Each SSID should be assigned a different VLAN. This will aid in separating traffic (staff from student from guest, for example). Each VLAN, as well, can be assigned a different IP scope.

Security

WPA2 Enterprise utilizes 802.1x authentication, providing security and assuring that only those devices and users that are allowed to connect to the network do so.

Radios

Make use of all the spectrum that you can. However, if there are more than five APs in close proximity, limit the number of 2.4 GHz radios that are enabled. For example, if there are 10 APs in a very large classroom, only enable 2.4 GHz on up to five of them, but enable 5 GHz on all APs.

Max Clients

This setting will limit the number of client devices that can connect to a single AP. The number used here will vary depending on the application requirements. For a theater-style classroom, our assumption is that high throughput is desired, with an assumed ideal of up to 60 clients per AP. By allowing for 25% over that number, we have provided some safety margin in case an AP was to fail.

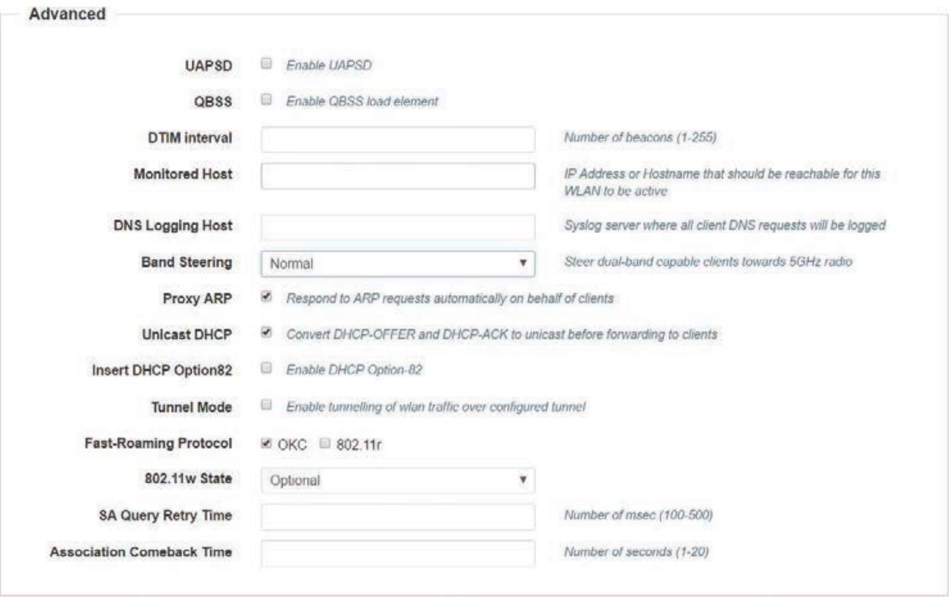
Client Isolation

Client isolation prevents clients on an AP from seeing or communicating directly with any other clients on that same AP. Think of this option as a way to protect clients from each other. Unless there is a need for client to client communications, enable this option. If there is a need to pass traffic between the professor/moderator and those in attendance, client isolation can still be used if the professor/moderator is connected to a different SSID on a different VLAN. Traffic must pass through a router in this case. Or, instead, an ACL can be applied that only allows two-way communication between the professor/moderator and those in attendance but not between attendees. ACLs will be covered later.

Drop Multicast Traffic

The assumption is made that multicast applications will be in use. If this is the case, this option should not be enabled. If it is not the case, enable this option to block unnecessary traffic.

Advanced WLAN Settings



Advanced

UAPSD	☐ Enable UAPSD	
QBSS	☐ Enable QBSS load element	
DTIM interval		Number of beacons (1-255)
Monitored Host		IP Address or Hostname that should be reachable for this WLAN to be active
DNS Logging Host		Syslog server where all client DNS requests will be logged
Band Steering	Normal ▾	Steer dual-band capable clients towards 5GHz radio
Proxy ARP	☑ Respond to ARP requests automatically on behalf of clients	
Unicast DHCP	☑ Convert DHCP-OFFER and DHCP-ACK to unicast before forwarding to clients	
Insert DHCP Option82	☐ Enable DHCP Option-82	
Tunnel Mode	☐ Enable tunnelling of wlan traffic over configured tunnel	
Fast-Roaming Protocol	☑ OKC ☐ 802.11r	
802.11w State	Optional ▾	
SA Query Retry Time		Number of msec (100-500)
Association Comeback Time		Number of seconds (1-20)

Band Steering

Enable band steering to help load balance properly between 2.4 and 5 GHz radios.

Proxy ARP

Enable Proxy ARP to help reduce broadcast traffic.

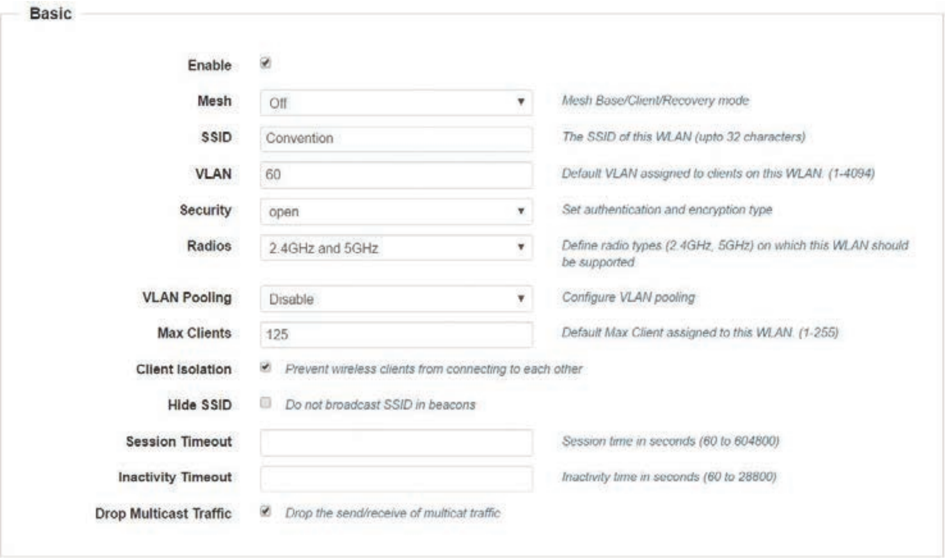
Unicast DHCP

Enable Unicast DHCP to direct DHCP broadcasted requests directly to the DHCP server.

Fast-Roaming Protocol

While roaming is not a primary concern for this type of deployment, enabling OKC will improve roaming performance while Radius servers are used for authentication (WPA2-Enterprise).

Convention Hall



Basic

Enable	☑	
Mesh	Off ▾	Mesh Base/Client/Recovery mode
SSID	Convention	The SSID of this WLAN (upto 32 characters)
VLAN	60	Default VLAN assigned to clients on this WLAN. (1-4094)
Security	open ▾	Set authentication and encryption type
Radios	2.4GHz and 5GHz ▾	Define radio types (2.4GHz, 5GHz) on which this WLAN should be supported
VLAN Pooling	Disable ▾	Configure VLAN pooling
Max Clients	125	Default Max Client assigned to this WLAN. (1-255)
Client Isolation	☑ Prevent wireless clients from connecting to each other	
Hide SSID	☐ Do not broadcast SSID in beacons	
Session Timeout		Session time in seconds (60 to 604800)
Inactivity Timeout		Inactivity time in seconds (60 to 28800)
Drop Multicast Traffic	☑ Drop the send/receive of multicat traffic	

Mesh

For high density deployments, it is best to avoid mesh where possible. Mesh forces two or more APs to utilize the same channel, and limits the capacity of those APs to that of a single one. In a Convention Hall, there should be no need to utilize mesh with the ability to connect Ethernet to each AP.

VLAN

While the use of VLANs is not strictly required, it is a good tool for separating traffic. Each SSID should be assigned a different VLAN. This will aid in separating traffic (staff from attendees, for example). Each VLAN, as well, can be assigned a different IP scope.

Security

The expectation is that a Captive Portal will be used for signing into the wireless network. That captive portal could be what is provided by Cambium, built into cnMaestro, or it could be an external portal, or even a third-party solution. In any of these cases, Open authentication is the most typical configuration for the SSID.

Radios

Make use of all the spectrum that you can. However, if there are more than five APs in close proximity, limit the number of 2.4 GHz radios that are enabled. For a Convention Hall, it is not unusual for 1/3 of the 2.4 GHz radios to be disabled while 100% of the 5 GHz radios are enabled.

Max Clients

This setting will limit the number of client devices that can connect to a single AP. The number used here will vary depending on the application requirements. For this use case, we are using a fairly typical ideal number of 100 clients per AP. By allowing for 25% over that number, we have provided some safety margin in case an AP was to fail.

Client Isolation

Client isolation prevents clients on an AP from seeing or communicating directly with any other clients on that same AP. Think of this option as a way to protect clients from each other. Unless there is a need for client to client communications, enable this option. In a Convention Hall it is not recommended to allow this type of communications.

Drop Multicast Traffic

The assumption is made that multicast applications will be in use. If this is the case, this option should not be enabled. If it is not the case, enable this option to block unnecessary traffic.

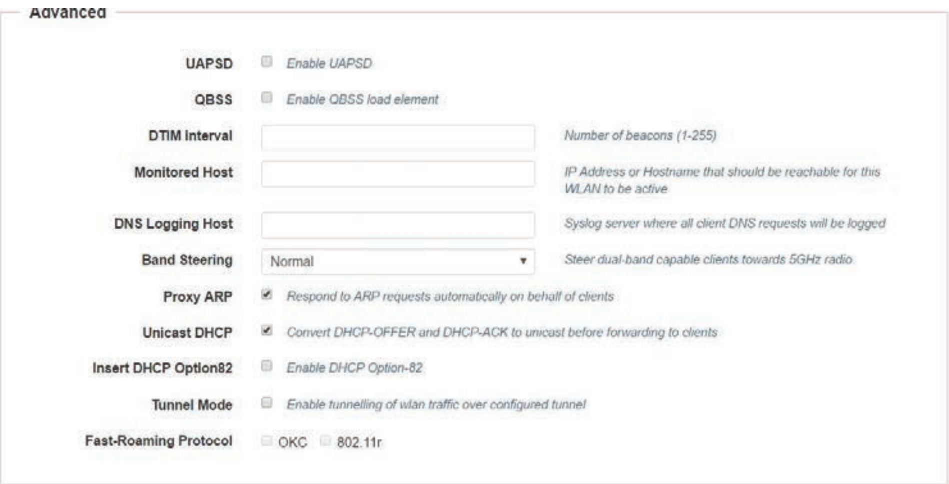
Advanced WLAN Settings

Band Steering

Enable band steering to help load balance properly between 2.4 and 5 GHz radios.

Proxy ARP

Enable Proxy ARP to help reduce broadcast traffic.



Advanced

UAPSD	□ Enable UAPSD	
QBSS	□ Enable QBSS load element	
DTIM Interval		Number of beacons (1-255)
Monitored Host		IP Address or Hostname that should be reachable for this WLAN to be active
DNS Logging Host		Syslog server where all client DNS requests will be logged
Band Steering	Normal ▾	Steer dual-band capable clients towards 5GHz radio
Proxy ARP	☑ Respond to ARP requests automatically on behalf of clients	
Unicast DHCP	☑ Convert DHCP-OFFER and DHCP-ACK to unicast before forwarding to clients	
Insert DHCP Option82	□ Enable DHCP Option-82	
Tunnel Mode	□ Enable tunnelling of wlan traffic over configured tunnel	
Fast-Roaming Protocol	□ OKC □ 802.11r	

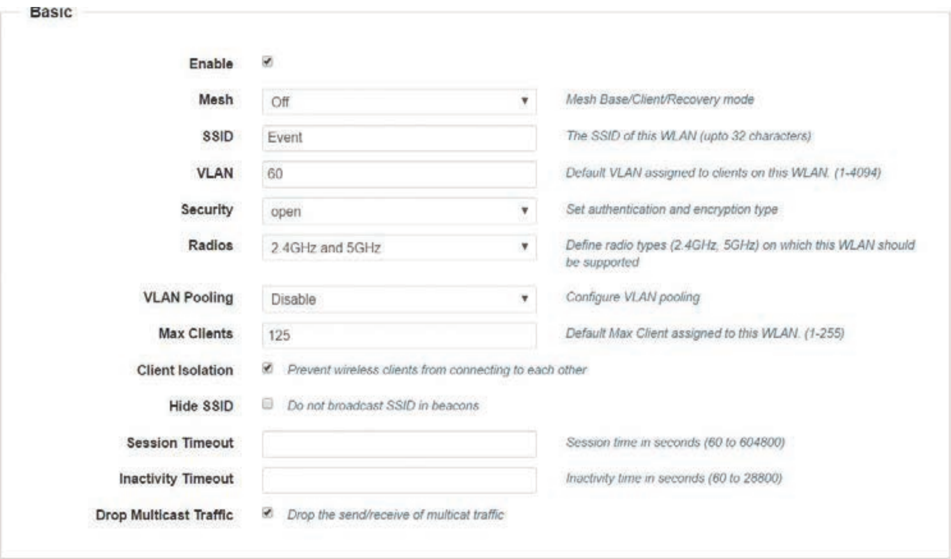
Unicast DHCP

Enable Unicast DHCP to direct DHCP broadcasted requests directly to the DHCP server.

Outdoor Event

Mesh

For high density deployments, it is best to avoid mesh where possible. Mesh forces two or more APs to utilize the same channel, and limits the capacity of those APs to that of a single one. Mesh can offer functionality that is needed in a deployment of this type. However, it is possible



Basic

Enable	☑	
Mesh	Off ▾	Mesh Base/Client/Recovery mode
SSID	Event	The SSID of this WLAN (upto 32 characters)
VLAN	60	Default VLAN assigned to clients on this WLAN. (1-4094)
Security	open ▾	Set authentication and encryption type
Radios	2.4GHz and 5GHz ▾	Define radio types (2.4GHz, 5GHz) on which this WLAN should be supported
VLAN Pooling	Disable ▾	Configure VLAN pooling
Max Clients	125	Default Max Client assigned to this WLAN. (1-255)
Client Isolation	☑ Prevent wireless clients from connecting to each other	
Hide SSID	□ Do not broadcast SSID in beacons	
Session Timeout		Session time in seconds (60 to 604800)
Inactivity Timeout		Inactivity time in seconds (60 to 28800)
Drop Multicast Traffic	☑ Drop the send/receive of multicat traffic	

to use PMP solutions to provide connectivity to APs that cannot connect directly to Ethernet otherwise. If PMP solutions are not used, enable Mesh, but only for those APs that would be using this function. At least one AP will need to be configured as a Base for mesh, with those that connect to it being configured as clients for mesh.

VLAN

While the use of VLANs is not strictly required, it is a good tool for separating traffic. Each SSID should be assigned a different VLAN. This will aid in separating traffic (staff from attendees, for example). Each VLAN, as well, can be assigned a different IP scope.

Security

The expectation is that a Captive Portal will be used for signing into the wireless network. That captive portal could be what is provided by Cambium, built into cnMaestro, or it could be an external portal, or even a third-party solution. In any of these cases, Open authentication is the most typical configuration for the SSID.

Radios

Make use of all the spectrum that you can. However, if there are more than five APs in close proximity, limit the number of 2.4 GHz radios that are enabled. For an Outdoor Event, it is not unusual for 1/3 of the 2.4 GHz radios to be disabled while 100% of the 5 GHz radios are enabled.

Max Clients

This setting will limit the number of client devices that can connect to a single AP. The number used here will vary depending on the application requirements. For this use case, we are using a fairly typical ideal number of 100 clients per AP. By allowing for 25% over that number, we have provided some safety margin in case an AP was to fail.

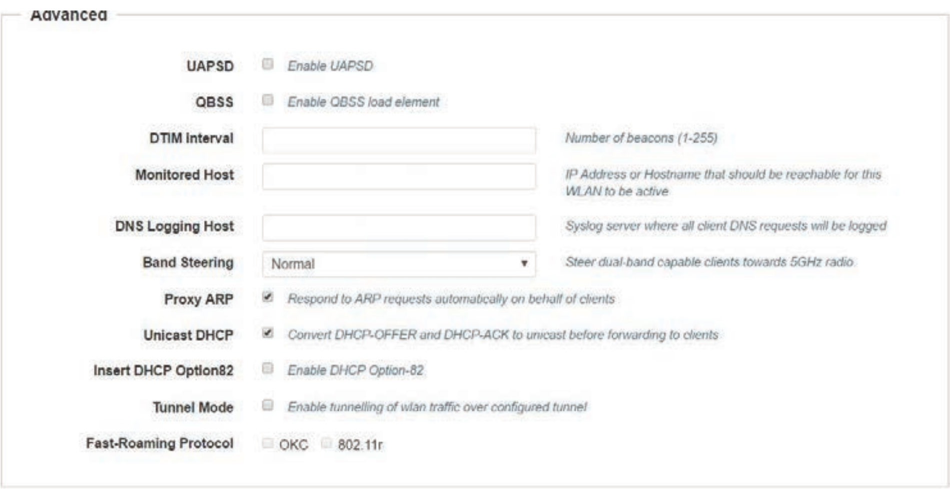
Client Isolation

Client isolation prevents clients on an AP from seeing or communicating directly with any other clients on that same AP. Think of this option as a way to protect clients from each other. Unless there is a need for client to client communications, enable this option. In an outdoor event it is not recommended to allow this type of communications.

Drop Multicast Traffic

The assumption is made that multicast applications will be in use. If this is the case, this option should not be enabled. If it is not the case, enable this option to block unnecessary traffic.

Advanced WLAN Settings



Advanced

UAPSD	☐ Enable UAPSD	
QBSS	☐ Enable QBSS load element	
DTIM Interval		Number of beacons (1-255)
Monitored Host		IP Address or Hostname that should be reachable for this WLAN to be active
DNS Logging Host		Syslog server where all client DNS requests will be logged
Band Steering	Normal ▾	Steer dual-band capable clients towards 5GHz radio
Proxy ARP	☑ Respond to ARP requests automatically on behalf of clients	
Unicast DHCP	☑ Convert DHCP-OFFER and DHCP-ACK to unicast before forwarding to clients	
Insert DHCP Option82	☐ Enable DHCP Option-82	
Tunnel Mode	☐ Enable tunnelling of wlan traffic over configured tunnel	
Fast-Roaming Protocol	☐ OKC ☐ 802.11r	

Band Steering

Enable band steering to help load balance properly between 2.4 and 5 GHz radios.

Proxy ARP

Enable Proxy ARP to help reduce broadcast traffic.

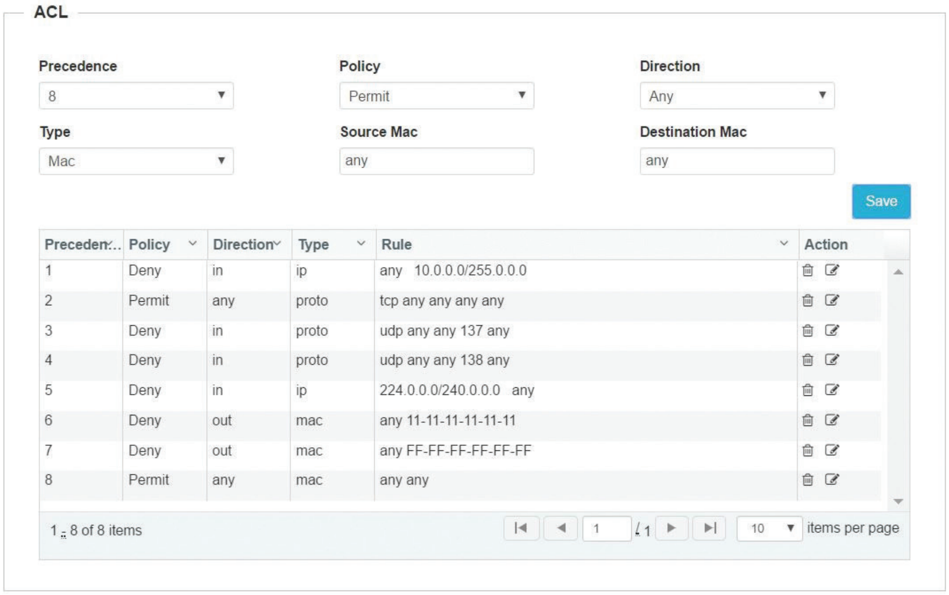
Unicast DHCP

Enable Unicast DHCP to direct DHCP broadcasted requests directly to the DHCP server.

WLAN ACCESS SETTINGS

ACLs

The use of ACLs applied to an SSID is twofold. First is to reduce unnecessary traffic. Second is to strengthen client isolation, protecting clients from each other. Below is an example where clients are assigned an IP address in the 10.0.0.0 DHCP scope and there is no need for IP multicast traffic to be supported.



ACL

Precedence	Policy	Direction
8 ▾	Permit ▾	Any ▾
Type	Source Mac	Destination Mac
Mac ▾	any	any

Preceden...	Policy	Direction	Type	Rule	Action
1	Deny	in	ip	any 10.0.0.0/255.0.0.0	🗑 ✎
2	Permit	any	proto	tcp any any any any	🗑 ✎
3	Deny	in	proto	udp any any 137 any	🗑 ✎
4	Deny	in	proto	udp any any 138 any	🗑 ✎
5	Deny	in	ip	224.0.0.0/240.0.0.0 any	🗑 ✎
6	Deny	out	mac	any 11-11-11-11-11-11	🗑 ✎
7	Deny	out	mac	any FF-FF-FF-FF-FF-FF	🗑 ✎
8	Permit	any	mac	any any	🗑 ✎

1 - 8 of 8 items

ACL Entries

ACLs are ordered by rule number. Once an ACL is defined, unless there is an explicit *allow*, all packets will be dropped. This is the reason for the final entry in this ACL list. Explanations of the others entries follows in the order in which they are listed above.

1. This entry block clients connected to the WLAN on a specific AP from addressing any other client on any other AP.
2. This entry allows all TCP traffic in both directions, essential to web surfing.
3. This entry allows DHCP requests from the clients out toward the DHCP server. Earlier, we also defined a setting that will have the AP change this DHCP request from broadcast to unicast, lessening the effect of broadcasts on the wire portion of the network.
4. This entry blocks some Windows Netbios traffic from clients.
5. This entry blocks the rest of the possible Windows Netbios traffic from clients.
6. This entry blocks IP multicast traffic from clients.
7. This entry block DHCP discovery packets from being sent out towards clients. DHCP discovery packets should only come from the clients and be sent towards the DHCP server.
8. This entry will block Cambium Networks inter AP communications packets from being seen by clients.
9. This entry prevents broadcasts from being sent out towards clients. Broadcasts such as DHCP requests from clients and ARP requests are allow in the other direction.
10. The last entry is required to allow all other traffic types.

ETHERNET

Ethernet port settings can also be used to block unnecessary traffic and provide some Firewall-like protection.

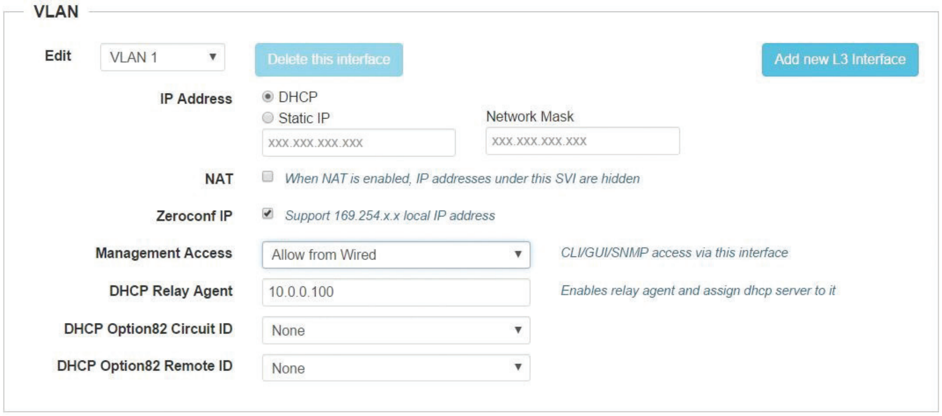
VLAN Settings

Management Access

Configuring this setting to "Allow from Wired" will allow management access to the AP through this VLAN without allowing it from wireless clients.

DHCP Relay Agent

Enter the IP address of the DHCP Server to allow the AP to direct DHCP request packets in unicast format.



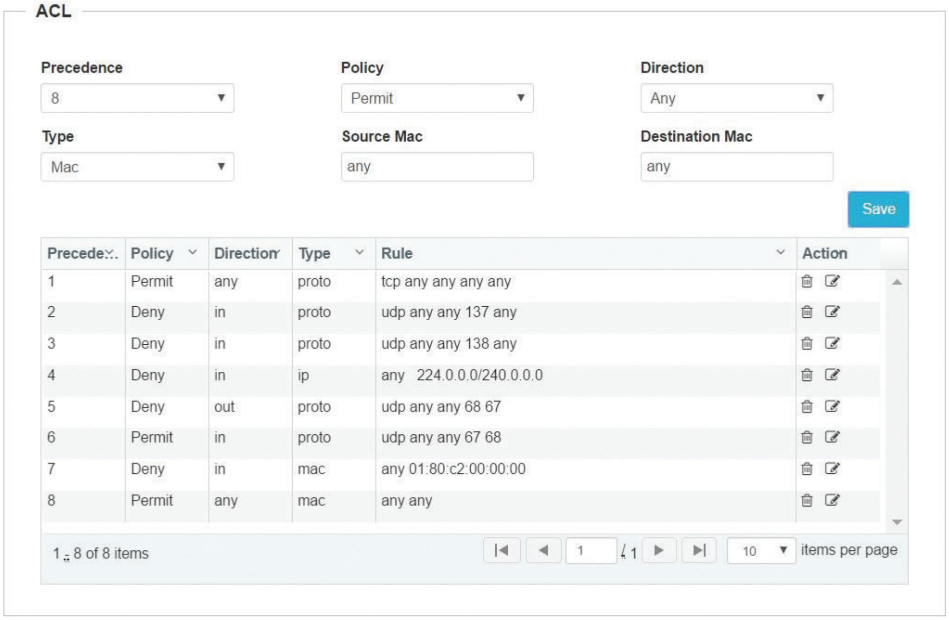
VLAN

Edit	VLAN 1 ▾
IP Address	● DHCP ○ Static IP xxx.xxx.xxx.xxx
Network Mask	xxx.xxx.xxx.xxx
NAT	□ *When NAT is enabled, IP addresses under this SVI are hidden*
Zeroconf IP	☑ *Support 169.254.x.x local IP address*
Management Access	Allow from Wired ▾ *CLI/GUI/SNMP access via this interface*
DHCP Relay Agent	10.0.0.100 *Enables relay agent and assign dhcp server to it*
DHCP Option82 Circuit ID	None ▾
DHCP Option82 Remote ID	None ▾

Ethernet Ports

Under this tab, you can configure ACLs for the Ethernet port. The example below shows a typical Ethernet ACL list. In the order that they are listed here is an explanation of each entry.

1. Allows all TCP traffic.
2. Blocks some Windows Netbios traffic.
3. Blocks the rest of the Windows Netbios traffic.
4. Blocks IP multicast traffic.
5. Blocks DHCP discoveries from the Ethernet port towards wireless clients.
6. Allows DHCP discoveries from wireless clients.
7. Blocks 802.1d packets from wired infrastructure out towards wireless clients.
8. Allows all other traffic.



ACL

Precedence	Policy	Direction
8 ▾	Permit ▾	Any ▾
Type	**Source Mac**	**Destination Mac**
Mac ▾	any	any

Precede…	Policy	Direction	Type	Rule	Action
1	Permit	any	proto	tcp any any any any	🗑 ✎
2	Deny	in	proto	udp any any 137 any	🗑 ✎
3	Deny	in	proto	udp any any 138 any	🗑 ✎
4	Deny	in	ip	any 224.0.0.0/240.0.0.0	🗑 ✎
5	Deny	out	proto	udp any any 68 67	🗑 ✎
6	Permit	in	proto	udp any any 67 68	🗑 ✎
7	Deny	in	mac	any 01:80:c2:00:00:00	🗑 ✎
8	Permit	any	mac	any any	🗑 ✎

1 - 8 of 8 items

PORTAL

The venue will want a Portal to be used by anyone accessing the Wi-Fi network. A portal will allow for differentiation in services, ensure Terms and Conditions are agreed upon, provide identification of the network to visitors, and allow for options such as advertising and links to applications that may be offered by the venue. Cambium offers a customizable portal built into cnMaestro™ at no extra charge with abilities such as Social Login, a Walled Garden, Vouchers, and Payment options. Third party portal services such as Encapto, Purple, Jaze, Vedicsoft, Cloud4Wi, and many others can provide even more options such as advertising and Location information. The configuration of these options is beyond the scope of this document. For information on configuring the portal offered by Cambium, please see more at our support web site https://support.cambiumnetworks.com. And for information on the configuration of 3rd party options, please see their respective support web sites.

OTHER NETWORK CONSIDERATIONS

ETHERNET SWITCHES

PoE

Make certain that PoE switches have enough capability to simultaneously power up all APs that connect through them.

MAC address tables

Make certain that all Ethernet switches have sufficient table sizes to handle enough MAC addresses. This must be true not just of the core switches but the edge switches as well.

Server Capacity

All back-end services must be scaled properly. This includes DHCP scopes and servers, DNS servers, Radius, and Portal capabilities.

Cambium Networks™

Cambium Networks, Ltd.
3800 Golf Road, Suite 360,
Rolling Meadows, IL 60008