Cambium Networks™

MAXIMIZING THE BENEFITS OF WI-FI FOR RESIDENTS

Wi-Fi Deployments in Multi-Dwelling Units (MDU)

MDUs have Wi-Fi needs that are unique in that they combine the elements of public Wi-Fi with private Wi-Fi. Furthermore, it is imperative that the Wi-Fi network provide adequate performance and be easy to access. MDUs vary in type and size, but the basic need is for good coverage, easy access, and separation of traffic. There are some variances in best practices between the different MDU types, but the basic design remains the same. In this document we will discuss each of the following topics:

- **MDU examples**
- MDU Wi-Fi needs and considerations
- The typical Wi-Fi design and MDU applications
- Recommended MDU Wi-Fi design
- cnPilot™ configuration
- cnPilot AP models and their uses in MDUs
- Captive Portal, RADIUS, and Ethernet switch considerations

MDU DEPLOYMENT EXAMPLES

APARTMENTS

Apartments are the most common example of MDUs and of all the examples that we will examine. This is the example with the highest user density. Depending on the size and complexity of the units, it may be possible to provide adequate coverage with traditional APs in hallways and common areas, covering more than one apartment per AP. However, a better design is to mount an AP within each unit.

One aspect of apartments that is quite important to a good Wi-Fi design is that there tends to be a fair amount of bleed through of Wi-Fi signal between units, both next to each other and from floor to floor.

TOWNHOUSES

Townhouses tend to be much larger units with fewer of them connected to each other. For this reason, unlike apartments, townhouses tend to be subject to less bleed through of Wi-Fi signal from one unit to another and can possibly be best treated as single dwelling units.

DORMITORIES

Dormitories are a unique example of an MDU. The residents change often. The users make heavy use of Wi-Fi, perhaps the heaviest of all these examples. And, last but not least, the density of both users and devices is the highest of all of the examples. Dormitory rooms can vary from tiny spaces to luxurious, but they do tend to be packed closer together than apartments, meaning that Wi-Fi signal bleed through will be high.

SENIOR AND ASSISTED LIVING

Senior living and assisted living facilities are an often overlooked MDU type. More and more are being built and those entering into these facilities are more active on the internet than ever before. Where Wi-Fi might not have been considered a necessity for this market in the past, it is now considered a basic utility. These facilities can vary as much as apartments and can be considered nearly identical for Wi-Fi needs and design with the exception that there are generally more common areas and more need for guest access.

BARRACKS

Military barracks can be considered as very similar to dormitories. Size and density of users are very similar. Also similar is the heavy use of Wi-Fi for gaming devices.

WI-FI NEEDS FOR MDUS

RESIDENTS

In each MDU case that we are examining, the residents are the most important. They also have the ability to provide their own Wi-Fi. The problem with this is, especially in the more dense deployments, that when residents start to implement their own solutions, there tends to be more problems with interference. If you provide poor Wi-Fi for the residents, they will add their own. That will, in turn make Wi-Fi even worse for everyone. It is in your best interest, and that of the residents, to provide excellent Wi-Fi to everyone.

ACCESSIBILITY

Access to the Wi-Fi network must be easy: easy to find, easy to connect, and easy to use. This includes all devices that residents use. That list is much longer than ever before with not only PCs and laptops, but also printers, TVs, AppleTV, Roku, Alexa, tablets, iPods, smart watches, refrigerators, thermostats, and surveillance cameras. Some of these devices utilize broadcast protocols such as bonjour and CUPS to advertise their services. This means that you cannot enable Client Isolation as you would for a guest network.

SECURITY

It is vital that each residential unit be protected from the users in other residential units. As we discussed previously, however, there is a real need to allow all devices within a residence to have free communications between them. Each residence needs to be treated as a unique and separate network. It is also important to prevent unauthorized users to access the network as they could take up bandwidth intended for the residents.

GUESTS

The choice to allow guest access should be considered, along with an implementation of how to limit that access to valid guest users and not just someone living or lurking close by. It is also important to limit guest access so that it does not impinge on bandwidth reserved for residents.

WI-FI NETWORK DESIGN

THE TRADITIONAL DESIGN

Traditionally, Wi-Fi in MDUs has been provided by using a home Wi-Fi/router in each unit. At first, this might seem to make the most sense. Each dwelling unit will have its own SSID and its own subnet. Traffic remains separated between the units, providing security for the residents from each other. However, there are definite drawbacks to this approach.

With a different SSID for each unit, there will be a very large number of them visible from any location throughout the complex. This can be confusing to the residents. It is also a lot for the Managed Service Provider (MSP) to manage.

Coverage for each unit is provided by an AP within each unit. For dormitories and barracks, this is generally not a large concern. However, with apartments, senior living, and townhomes, there will be locations within a resident's unit where they will have better signal strength from the AP inside their neighbor's unit.

If Wi-Fi is to be provided to common areas, it will be necessary to have an additional SSID present in those areas. Keep in mind that for every SSID, beacons are broadcasted by each AP. With only 4 different SSIDs present on the same channel being seen by 4 different APs, over 50% of the airtime is used by these beacons alone. That means that ½ of the possible capacity is being used by beacons. It is always better to reduce the number of beacons to as few as it possible.

A BETTER DESIGN

Cambium Networks offers offer a better design, one that simplifies connectivity for residents, protects their security, maximizes airtime, and also eases network management for the MSP. Instead of deploying a separate SSID for each unit, use a single SSID for the entire complex. If APs are placed within each unit, they will provide coverage to neighboring tenants. Devices will connect to the best possible AP in all cases. Even common areas are provided for with this single SSID.

MSPs should also separate traffic into a unique VLAN for each dwelling unit. All of the PCs, AppleTVs, smart watches, iPhones, TVs, etc that are owned by a single residence are placed on the same VLAN. By doing this, residents can use their printers and can watch Netflix, but they cannot see their neighbors' devices and traffic.

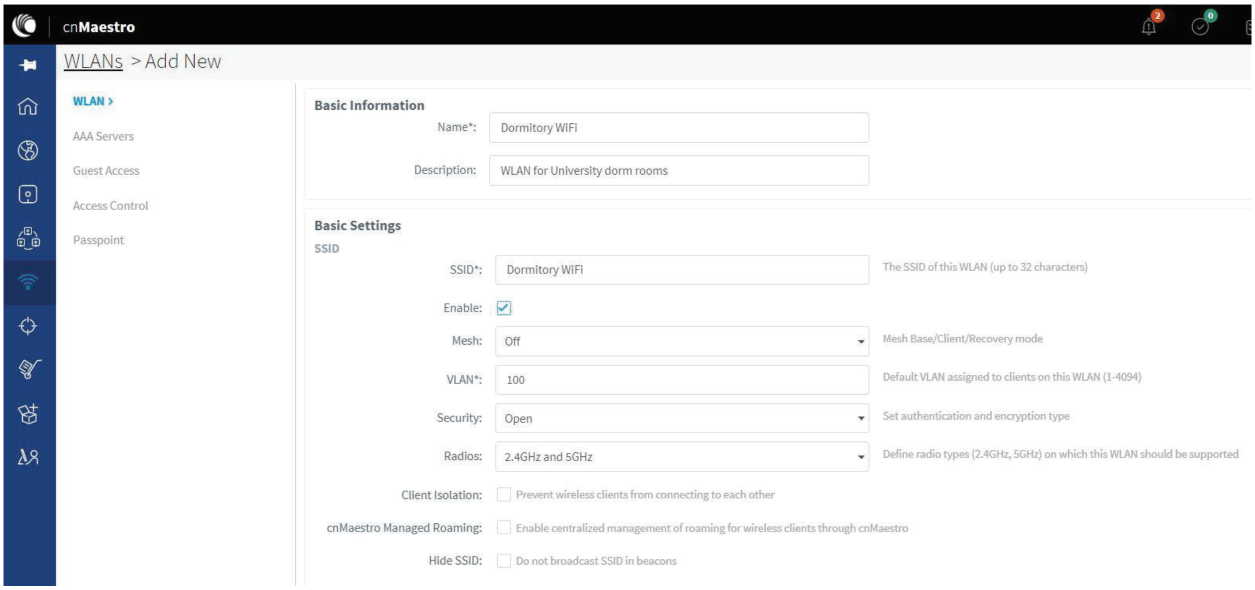
But how do you make this process simple? The key is to use a captive portal in conjunction with RADIUS MAC authentication and dynamic VLANs. When a resident first connects to the Wi-Fi network, they should be redirected to a captive portal where they can be verified as a resident. The captive portal should then allow residents to self-register their other devices. Not all Wi-Fi devices have a browser that can use a captive portal, so it is important to provide a method for adding those devices into the system. The captive portal then updates the RADIUS database, assigning a single and unique VLAN to all of the devices registered for a single residential unit. Once this is complete, a CoA (Change of Authentication) message is sent to the AP where the user is connected telling the AP to disconnect the client device. The device will immediately attempt to reconnect, but this time it will be assigned to the VLAN specified by the RADIUS server. All devices are now connected on their own private network within the same SSID. By placing each VLAN within a unique subnet, the network operator can also provide all of the bandwidth restrictions desired as well as firewall services to each residence.

REGISTRATION PROCESS

- Each new user connects to Wi-Fi with a browser capable device and is placed in "safe" VLAN
  - AP passes MAC address to RADIUS server for authentication
  - RADIUS server allows authentication but retains default (safe) VLANID
- The user is redirected to captive portal and asked for login credentials
  - The captive portal updates RADIUS database with user device MAC and assigned a unique VLANID
  - User is given the opportunity to enter the MAC address of other devices, to include headless devices
    - AppleTV/Roku
    - Gaming consoles
    - Printers
  - Added device MAC addresses are updated to RADIUS database along with dwelling unit VLANID
- CoA message sent to AP
  - User device disconnects and then reconnects with the new VLAN
  - All devices in a single dwelling unit share the same VLANID unique to that unit

cnPILOT CONFIGURATION

In order to configure cnPilot for this better design, you will need to configure the WLAN used specifically for RADIUS MAC authentication with CoA capabilities. The simple steps shown below for configuration are all done through the cnMaestro™ management system. While it is possible to also configure the same functions through the AP GUI, it makes more sense to also take advantage of the MSP features offered by cnMaestro such as reporting, multi-tenancy, and AP grouping.



WLANs > Add New

Basic Information

Name*: Dormitory WiFi

Description: WLAN for University dorm rooms

Basic Settings

SSID

SSID*: Dormitory WiFi — The SSID of this WLAN (up to 32 characters)

Enable: ☑

Mesh: Off — Mesh Base/Client/Recovery mode

VLAN*: 100 — 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

Client Isolation: ☐ Prevent wireless clients from connecting to each other

cnMaestro Managed Roaming: ☐ Enable centralized management of roaming for wireless clients through cnMaestro

Hide SSID: ☐ Do not broadcast SSID in beacons

NEW WLAN

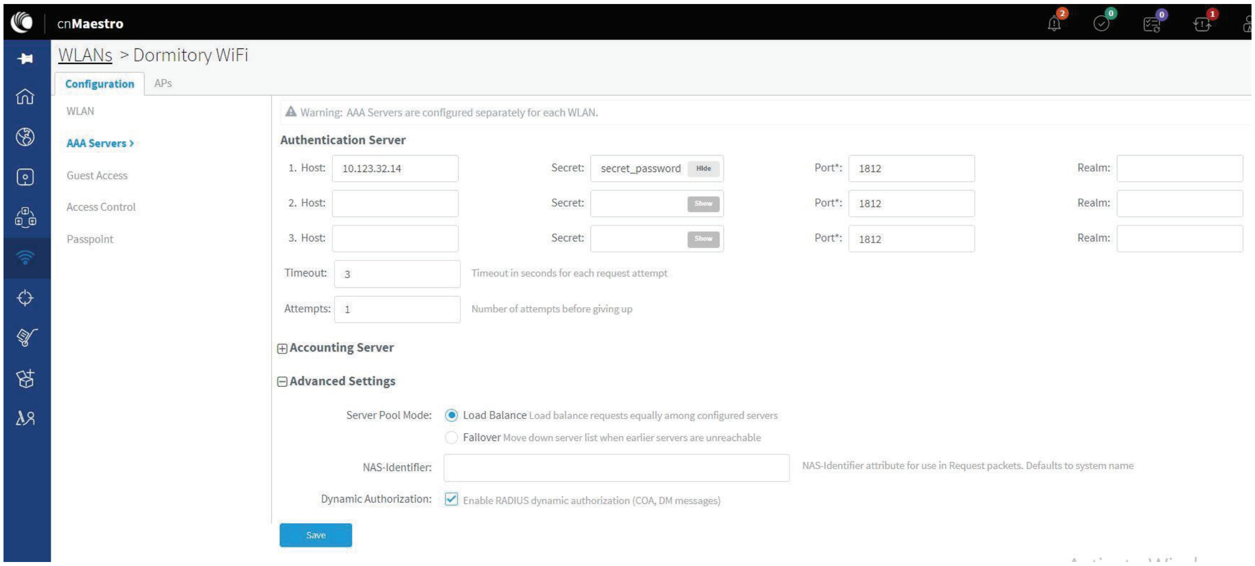
First, configure a new WLAN through the WLAN → New WLAN screen within cnMaestro.

Do not enable Client Isolation as that will prevent communications between devices such as an AppleTV and the TV. We also do not recommend hiding the SSID as you want connecting to the Wi-Fi network to be as simple as possible for the residents. Remember, if it becomes difficult, residents will start to deploy their own Wi-Fi equipment. This, in turn, will denigrate the quality of the Wi-Fi experience for everyone else by adding interference and complexity.

Note the use of a VLAN definition in this example. Clients that connect for the first time will be assigned to this VLAN. Configure this VLAN within your network to have access to the captive portal, and to support DHCP and DNS. However, do not allow Internet access. This will be a “safe” VLAN where first time users are temporarily housed until they complete the registration process.

AAA CONFIGURATION

It will be necessary to utilize a RADIUS server for MAC authentication. The RADIUS server will not only track the MAC addresses of residents’ devices, but will also be used to assign VLANs and to issue CoA messages during the registration process. At this time, cnMaestro does not provide a RADIUS server. However, there are various good options on the market, some of which are free to use such as FreeRADIUS (https://freeradius.org). Configure the AAA service IP address, shared secret, and enable CoA within the WLAN on cnMaestro under the AAA Servers options for the WLAN that you are configuring.



WLANs > Dormitory WiFi

⚠ Warning: AAA Servers are configured separately for each WLAN.

Authentication Server

1. Host: 10.123.32.14 Secret: secret_password Port*: 1812 Realm:
2. Host: Secret: Port*: 1812 Realm:
3. Host: Secret: Port*: 1812 Realm:

Timeout: 3 Timeout in seconds for each request attempt

Attempts: 1 Number of attempts before giving up

⊞ **Accounting Server**

⊟ **Advanced Settings**

Server Pool Mode: ● Load Balance Load balance requests equally among configured servers
○ Failover Move down server list when earlier servers are unreachable

NAS-Identifier: NAS-Identifier attribute for use in Request packets. Defaults to system name

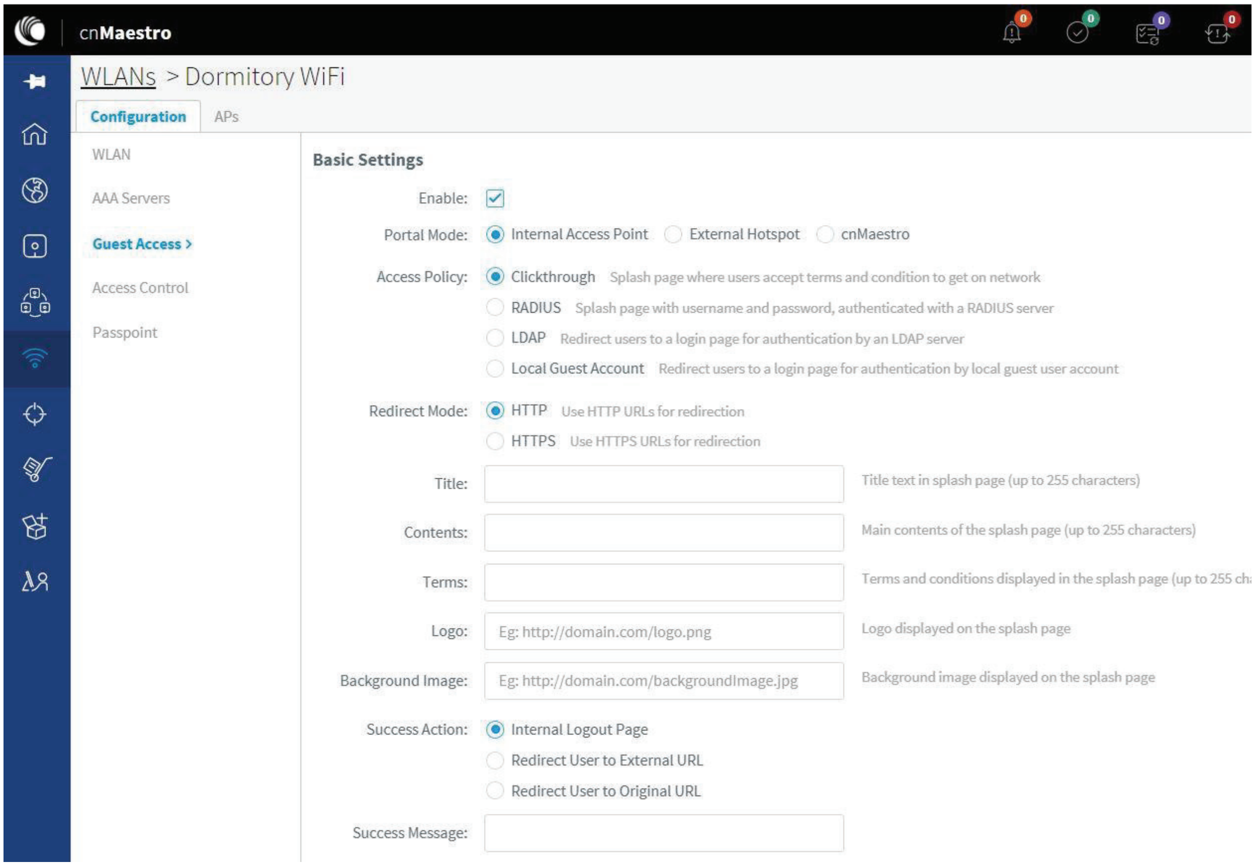
Dynamic Authorization: ☑ Enable RADIUS dynamic authorization (COA, DM messages)

Check the box for Dynamic Authorization. This will enable the APs to which this WLAN is assigned to understand and accept CoA and DM messages (Change of Authorization and Disconnect Message).

GUEST ACCESS

Next, you will want to configure Guest Access information for the WLAN, pointing to the external captive portal that will integrate with your RADIUS server. Although cnMaestro does offer a customizable Guest Access portal, it does not have the ability to fully integrate with a RADIUS server to the extent that is required for this type of deployment. There are options on the market for a captive portal that will integrate with cnPilot APs and cnMaestro such as the rXg offered by RG Nets (www.rgnets.com). RG Nets offers this versatile solution as either a physical appliance or as a virtual machine, both with the RADIUS server built into it. If you have a capable staff, it may also be possible to write your own captive portal for this functionality.

Configure the information needed to redirect first time users to the external captive portal.



Basic Settings

Enable: ☑

Portal Mode: ● Internal Access Point ○ External Hotspot ○ cnMaestro

Access Policy:
● Clickthrough Splash page where users accept terms and condition to get on network
○ RADIUS Splash page with username and password, authenticated with a RADIUS server
○ LDAP Redirect users to a login page for authentication by an LDAP server
○ Local Guest Account Redirect users to a login page for authentication by local guest user account

Redirect Mode:
● HTTP Use HTTP URLs for redirection
○ HTTPS Use HTTPS URLs for redirection

Title: Title text in splash page (up to 255 characters)

Contents: Main contents of the splash page (up to 255 characters)

Terms: Terms and conditions displayed in the splash page (up to 255 ch

Logo: Eg: http://domain.com/logo.png Logo displayed on the splash page

Background Image: Eg: http://domain.com/backgroundImage.jpg Background image displayed on the splash page

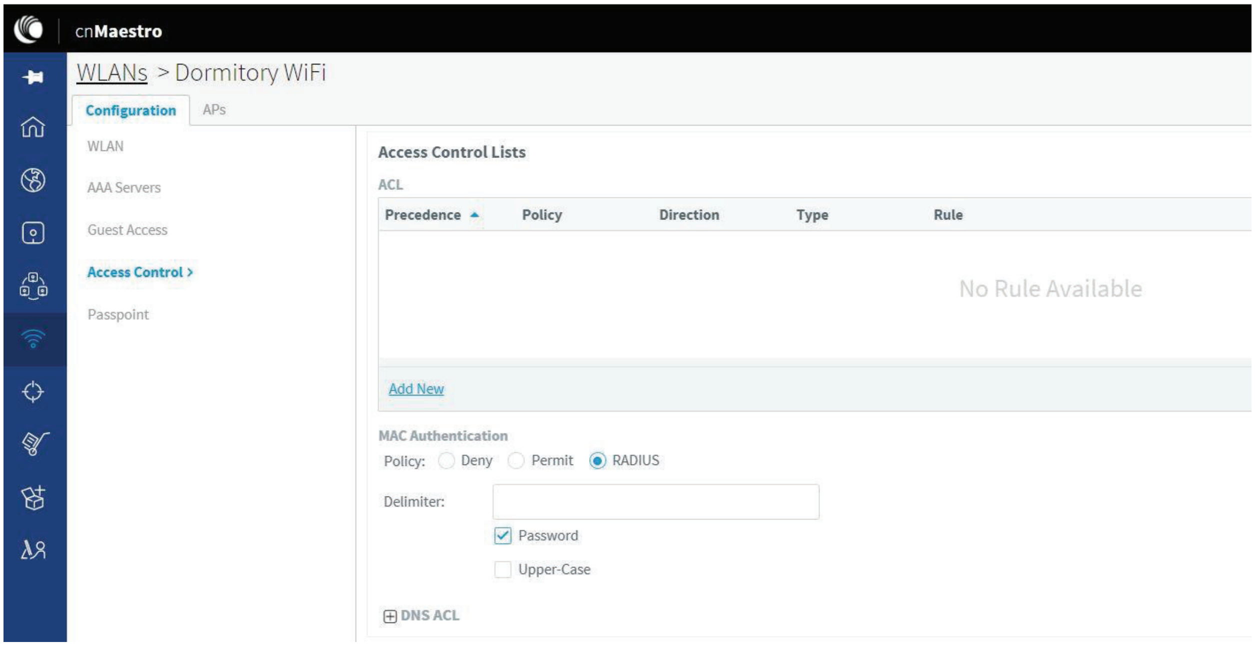
Success Action:
● Internal Logout Page
○ Redirect User to External URL
○ Redirect User to Original URL

Success Message:

In this example we show the use of HTTPS. While this is not strictly required, it is a good security practice. Tech savvy users will also insist on using HTTPS for any websites that request login information.

ACCESS CONTROL

The last portion of the WLAN configuration is for Access Control and is found under WLAN → Access Control for the specified WLAN. In this section, you will configure the WLAN to utilize RADIUS MAC authentication. This will tell the AP to send information such as the MAC address as well as the framed IP address to the RADIUS server.



Access Control Lists

ACL

Precedence ▲	Policy	Direction	Type	Rule

No Rule Available

MAC Authentication

Policy: ○ Deny ○ Permit ● RADIUS

Delimiter:

☑ Password

☐ Upper-Case

Most RADIUS server implementations have the ability to access any typical delimiter (:, -, and even a space) as well as to accept both upper and lower case characters. If your implementation requires a specific delimiter or differentiates between upper and lower case characters, be certain to configure this form appropriately.

OTHER CONSIDERATIONS

AP MODELS

e430W

The e430W is the workhorse for MDU deployments. This AP comes in a wallplate

format and is a 2x2:2 802.11ac wave 2 dual-band AP. It is powered via either 802.3af PoE or DC power and it can either be mounted on the wall or used with a stand.

Besides the input Ethernet port there is also a pass-through RJ-45 input and output as well as 3 other Ethernet output ports. Each output Ethernet port can be configured for different VLANs. This AP is uniquely well designed for MDUs and a single unit can provide sufficient coverage for a typical dormitory room, barracks

room, hotel room, and even many apartments and senior living units. It can provide both wired and wireless access. MSPs providing services for MDUs might be interested in expanding their service offerings to IPTV. The added Ethernet ports can provide connectivity for IPTV and even IP phone systems, significantly reducing installation costs by reducing the number of Ethernet drops required per unit to one.

e410

The e410 is an indoor 802.11ac 2x2 wave 2 dual-band AP. For deployments where the design involves providing coverage from the common areas, such as hallways, rather than placing one AP in each unit, this will be the one most commonly used. The e410 is power via 802.3af PoE and is small and unobtrusive.

e600

The e600 is an indoor 802.11ac 4x4 wave 2 dual-band AP. This AP is capable of much higher capacity than the e410 and is more ideally suited for areas where a large number of people are likely to gather, such as conference and party rooms. This AP can also be powered via 802.3af PoE, but will be limited to 17 dBm output power on the 5 GHz side unless 802.3at PoE+ is used.

e500 and e501s

The e500 and e501s are outdoor 802.11ac wave 1 2x2 dual-band APs. They include an IP67 enclosure to handle adverse weather conditions and they are powered via either 802.3af PoE or 802.3at PoE+. If 802.3at power is used, a second Ethernet port can be utilized to provide connectivity and power to another e500/501s, a camera, or any other device that requires 802.3af power. The difference between these two units is the antenna design. While the e500 has a 5 dBi omni-directional antenna, the e501s has a 120 degree 11 dBi antenna for greater range and more focused coverage. Both of these are good choices for outdoor areas to be covered such as poolside, picnic areas, and athletic fields.

Captive Portal

The captive portal plays an important role in this design. While cnMaestro does provide a guest access portal that can be customized in many ways, it does not currently offer the ability to allow users to self- register headless devices. For this, Cambium Networks recommends looking towards other products on the market, such as the rXg from RGNets (www.RGNets.com). This solution provides not only the self- registration portal, but also an integrated RADIUS server and has been tested and proven to work with the cnPilot product line.

RADIUS

A RADIUS server is also an integral part of this solution. There are many choices for a RADIUS server and any one of them should be usable as there are no aspects of this deployment that do not meet the standard functionality of a RADIUS server. FreeRADIUS (https://freeradius.org) is a free solution with significant documentation and forum support online, but can be a bit daunting for the uninitiated.

Microsoft's NPS requires a license, but offers a more friendly graphical interface.

Ethernet Switches and the Core Network

As dynamic VLANs will be used, there can be a significant number of VLANs that must be supported on the Ethernet switches deployed. Be certain to use Ethernet switches that can support as many VLANs as residential units for which they provide connectivity. Keep in mind that users may roam to any area of the complex. This means that at any one point in time, any Ethernet switch may need to support a larger number of VLANs than residential units that are connected directly to them. This is especially true of those switches that provide connectivity to APs covering common areas.

Although DC power can be used for the e430W wallplate APs, a more convenient deployment strategy is to use PoE switches to provide both connectivity and power to those APs. The e410, e600, and both models of the e50x line also require PoE.

With multiple VLANs comes multiple IP subnets. Routing can either happen at the complex, or be carried back to the MSP's core network. There is no reason to not use NAT, in fact this is likely to be the most commonly used method for providing IP addressing to all of the VLANs. Communications between the APs and cnMaestro is via TCP port 443, or HTTPS, which is not affected by NAT and is already allowed by any firewalls where internet access is required.

Cambium Networks™

India Office

Cambium Networks Consulting Private Ltd
5th Floor, Quadrant 1, Umiya Business Bay, Tower 2,Outer Ring Road,
Kadubisenahalli, Varthur Hobli Road, Bangalore East
Taluk, Bangalore- 560037
+91 80 67333100

San Jose Office

2590 N. 1st Street, Suite 220
San Jose, CA 95131 USA

US Office

3800 Golf Road, Suite 360
Rolling Meadows, IL 60008 USA
+1 888 863 5250

UK Office

Unit B2, Linhay Business Park
Eastern Road Ashburton, United Kingdom, TQ13 7UP
+44 1364 655500