Meru Networks®
Powering the All-Wireless Enterprise™

AP110 and AP1014i Deployment Guide

February 2013

Contents

Introduction

The AP110 and AP1014i are single-radio 802.11n wireless access points designed for data, voice, and video applications in enterprise-class, virtual office deployments with wired and wireless interfaces.

Plug-and-play deployment makes it easy to provide access to corporate networks to employees in branch offices or home offices, or to give guests in large hospitality segments, the ability to connect from their rooms. Wired ports provide secure connectivity for a VoIP phone or other wired devices, and built-in VPN encryption allows the access point to tunnel back data securely to the central controller from any internal remote network. Plug-and-play deployment eliminates the need for a costly, separate VPN infrastructure and reduces support costs. The savings scales with the number of devices per mobile user. For example, a telecommuter might require VPN security for a laptop, tablet, and smartphone. The AP110 and AP1014i can provide VPN security for all of a user's mobile devices.

As with all other Meru access points, the AP110 and AP1014i integrate seamlessly with Meru controllers and System Director, Meru's wireless operating system. Meru's management tools bring intelligent management and traffic control to your network. They support bandwidth-intensive applications, maximizing productivity for remote workers.

The AP1014i shares a similar hardware specification as an AP110, with the addition of four Fast Ethernet ports. The physical appearance of an AP1014i is the same as an AP1010 model with the integrated antenna. The AP110 and AP1014i support mesh and Meru's virtualization technology for Virtual Cell and Virtual Port.

The AP110 is supported on Meru System Director Release 5.2 or later, and the AP1014i is supported on System Director Release 5.3 or later. This guide is based on System Director Release 5.3.

What's Changed in this Document

The information about how the AP110 and AP1014i interact with the AP1010 and AP1020 was updated in Virtual Cell and Virtual Port.

About the AP110 and AP1014i

The AP110 and AP1014i share the same hardware specification, with the exception of the number of Ethernet ports supported. Table 1 lists the AP models and their wired and wireless interface characteristics.

Table 1: AP110 and AP1014i Models

Model	Wireless	Wired
AP110	Single-radio 802.11b/g/n: 2:2x2	Two interfaces: 10/100BASE-T
AP1014i	Single-radio 802.11b/g/n: 2:2x2	Five interfaces: 10/100BASE-T

The USB interface available on the APs is not currently used. The hardware reset button reset the entire configuration for an AP. No serial console interface is provided on the AP110 or AP1014i. The WPS push button on the AP110 is not currently supported.

For information about key features of the AP110 and AP1014i, see Key Features. For examples of how the AP110 and AP1014i can be deployed, see AP110 and AP1014i Deployments.

Key Features

The AP110 and AP1014i include the following features:

- Virtualization Support
- VPN
- Wired Client Support
- Mesh

Virtualization Support

The AP110 and AP1014i support virtualization, which offers the ability to optimize client-to-AP associations. Virtualization ensures that clients are always connected at the highest possible data rates and offers other benefits, such as seamless roaming and greater application performance and predictability.

The major advantage of virtualization is that each client device thinks that it is connected to the same AP, regardless of where the device is located or how often it roams between multiple APs. This takes away the decision-making capabilities of the client device when making inter-AP roaming decisions, which centralizes all control to the WLAN. The WLAN makes decisions about connectivity for client devices and allows users to change locations without disruptive handoffs.

The AP110/AP1014i access points support two types of virtualization:

- Virtual Cell (also known as shared BSSID)

  In this mode of virtualization, all APs advertising a particular SSID broadcast the same BSSID across the WLAN for that SSID. Virtual Cell is the default virtualization mode for System Director Release 5.3 or later.

  Different client chipset vendors incorporate different calculation methodologies for deciding when to roam from one AP to another. From a network perspective, this situation leads to inconsistency among various client devices and their behavior when it comes to roaming between two APs. This scenario is typical of why legacy microcell WLAN architectures have problems, especially in a BYOD environment.

- Virtual Port (also known as per-station BSSID)

  In this mode, a common parent BSSID (PBSSID) is broadcast for a particular SSID by all APs advertising that SSID. In Virtual Port, all clients receive a unique beacon and a unique broadcast/multicast key, making them invulnerable to certain types of key attacks. Each client is assigned its own BSSID. The BSSID remains the same for this particular client regardless of which AP the client is connected to.

For information about best practices for each virtualization mode, see the Best Practices Guide for High-Density Design and Deployment.

VPN

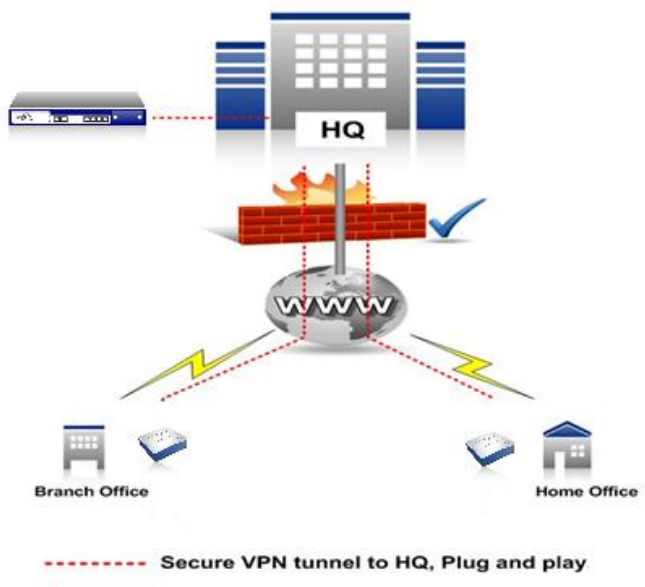
In the current Meru wireless system architecture, communication between the controller and AP takes place across specific UDP ports such as 5000, 9292, and 9393. It includes discovery of controller, communication between Meru applications on controller and AP, and data packet flow between different applications. All communication occurs over a UDP-encapsulated tunnel regardless of whether the controller and AP are located within the same network or on different networks. Some administrative overhead is added at times to open the firewall holes to allow traffic in enterprise networks while data travels across geographical boundaries.

The VPN feature provides a secure tunnel between the controller and AP as needed to ensure the security of traffic between them. With VPN enabled, all types of communication occur inside a secure channel. SSL VPN is used to implement the VPN server and client on controller and AP, respectively. The server and client together set up the secure VPN tunnel. The SSL (v3)/TLS (v1) VPN implementation provides encryption of communication data within the tunnel. AES-CBC (AES in Cipher Block Chaining mode) is the encryption algorithm used, which uses a 128-bit default key. TLS authentication (SHA1 algorithm) is used, which involves exchanging X.509 certificates for mutual authentication between the server (controller) and client (AP). The tunnel between the controller and AP is established using UDP port 1194, which is the well-known port for SSL VPN.

The VPN feature is available in System Director Release 5.3 or later.

Figure 1 illustrates a scenario in which users access corporate resources from home or a remote branch office. The built-in VPN functionality of the APs helps avoid making firewall changes and provides seamless access to the corporate network.

Figure 1: VPN Access to the Corporate Network



Wired Client Support

The AP110 and AP1014i support wired clients using wired interfaces. This feature provides connectivity, management, and monitoring for wired interfaces on Meru APs and wired clients that are connected to those wired interfaces. The wired stations go through the same assignment process from the controller as wireless clients do. The traffic from wired stations of an AP can be tunneled to a controller or can be bridged in a local AP network. This feature allows you to connect wired devices in any location in which adding more cable drops is difficult. The mesh backhaul on APs provides the additional capability of expanding networks with no cables. Additional information is provided in Wired Port Profiles.

Mesh

The mesh capability of the AP110 and AP1014i allows the extension of WLAN coverage in enterprises in which laying physical cables is costly or impractical. The mesh APs are able to communicate with the rest of the network by using wireless backhaul links rather than wired Ethernet.

The mesh feature is available in System Director Release 5.3 or later.

The AP110 and AP1014i are single-radio, 2.4 GHz-only devices and can only be leaf nodes in a mesh cloud, which means that the AP uses a wireless backhaul to connect to the controller but does not support wireless backhaul for any other nodes and client share the backhaul bandwidth. The AP can join a mesh cloud without special configuration (out of box), as it automatically finds the controller wirelessly when the controller Ethernet discovery fails.

More information about mesh is provided in Design Examples.

AP110 and AP1014i Deployments

The following are use cases, or deployment scenarios, in which the AP110 and AP1014i can be implemented:

- Use Case 1: Using the AP110 as a Telecommuter AP for the Home Office
- Use Case 2: Using the AP1014i as a Telecommuter AP for the Home Office
- Use Case 3: Branch Office Deployments
- Use Case 4: In-Room AP for Wireless and Wired Service
- Use Case 5: Leaf AP in a Mesh Cloud

Use Case 1: Using the AP110 as a Telecommuter AP for the Home Office

A telecommuter AP is an AP that a corporation provides to its employees for use at home. The AP connects to a controller at the corporate office and provides secure corporate network connectivity using VPN at the employee's home. The telecommuter AP can provide wireless access in tunneled mode (corporate) or bridged mode (personal). In many telecommuter offices, there is also a need to provide corporate connectivity for wired devices. The most common example is a VoIP phone that is connected to the corporate network and uses a standard corporate extension. The additional Ethernet port on the AP can be used to connect the wired devices and tunnel traffic to the corporate network.

For the design guidelines used in this use case, see Use Case 1 Design Example: Using the AP110 as a Telecommuter AP for the Home Office.

Use Case 2: Using the AP1014i as a Telecommuter AP for the Home Office

In addition to the scenario described in Use Case 1, a telecommuter AP is convenient for telecommuters who travel and can use the AP wherever an Internet connection is available. The additional wired interfaces in the AP1014i makes it easier to deploy in locations in which there is only a single Ethernet cable drop available that is already in use. Multiple devices can be connected to the wired interface of the AP1014i and can be tunneled back to corporate network or bridged locally according to the requirement. A typical example is to use a printer and a phone which is part of a tunneled port-profile and part of the same VLAN as the secure wireless SSID. This makes it easy for the corporate user to print documents while connected to corporate network.

For the design guidelines used in this use case, see Use Case 2 Design Example: Using the AP1014i as a Telecommuter AP for the Home Office.

Use Case 3: Branch Office Deployments

For companies with small branches in various locations, deploying and maintaining wireless networks can be expensive, and supporting many remote users can potentially overwhelm IT resources and operational budgets. The AP1014i simplifies the logistics of the staging process of remote offices with its built-in VPN capability. There are no traditional problems like restaging or reshipping materials. After the AP is VPN-enabled, the plug-and-play installation allows branches to virtually come up by themselves without requiring costly on-site wireless technicians. With a switch plugged in to the wired interface of the AP, additional wired devices can be supported. A bridged SSID for wireless traffic and a bridged port profile provide seamless access to local network resources for wireless and wired users. There can still be a secure tunneled SSID to be in use for corporate employees visiting the branch offices.

For the design guidelines used in this use case, see Use Case 3 Design Example: Branch Office Deployments.

Use Case 4: In-Room AP for Wireless and Wired Service

In many hotels, APs are usually placed in the hallways adjacent to guest rooms. The performance of the wireless network is often a problem when many users share or connect to the same access point. Coverage becomes challenging because the APs must be placed to provide adequate RSSI across guest rooms. With the AP110 and AP1014i supporting Meru Virtualization, there is no need for complex channel planning and site survey as APs can be placed in each guest room, which adds more capacity. The support of wired interfaces on the AP110 and AP1014i is also an advantage because there is no need to run extra cable drops to each room. Multiple wired devices can be connected to the wired interface, and the data can be intelligently switched through the central Meru controller.

For the design guidelines used in this use case, see Use Case 4 Design Example: In-Room AP for Wireless and Wired Service.

Use Case 5: Leaf AP in a Mesh Cloud

In addition to the scenario described in Use Case 4, the enterprise mesh capability of the AP110 and AP1014i extends wireless coverage in public areas of hotels (for example, pools and garden areas), where pulling Ethernet cables is nearly impossible. Once powered on, the APs establish wireless backhaul automatically with the next-hop AP in the mesh cloud. The APs are also capable of establishing redundant links in the event of connectivity failure with the parent AP (next-hop).

For the design guidelines used in this use case, see Use Case 5 Design Example: Leaf AP in a Mesh Cloud.

Design Guidelines

Consider the following when designing networks with the AP110 and AP1014i:

Differences Between the AP110 and AP1014i

As previously mentioned, the AP110 and AP1014i share the same hardware specifications, so their feature functionality and performance are similar. This sometimes makes it challenging to differentiate the AP models.

The following are some key differentiators to keep in mind while reading the use cases in this guide:

- The AP110 has a small form factor, which makes it ideal for telecommuters. The AP1014i has the same physical dimensions as an AP1010 access point.

  The AP1014i might not be a good recommendation as a telecommuter AP for a VPN use case. Having the same physical dimensions and mounting options of a standard AP1010 access point, the AP1014i is best deployed after onsite studies and consideration of mounting options (for example, below the table or above a false ceiling).

- The AP110 does not support PoE; the AP1014i supports PoE.

  The AP110 power overhead is marginal to a telecommuter use case, but might not be as practical as the AP1014i for hotel in-room deployment, as the AP110 requires a DC power source at each location. The AP1014i, however, will require factoring in the cost of an additional PoE injector at a location with no cable.

- The AP1014i has additional Ethernet ports, and the AP110 has a single interface.

  Keep in mind that performance is the same for wired and wireless users for both AP models. This means the recommended numbers of wired and wireless stations supported by both models are still same.

Virtual Cell and Virtual Port

In addition to Native Cell mode (non-virtualized mode), the AP110 and AP1014i support the following virtualization modes:

- Virtual Cell (also known as shared BSSID)
- Virtual Port (also known as per-station BSSID)

The AP110 and AP1014i cannot participate in a Virtual Cell with AP1010 and AP1020 access points.

For information about virtualization modes, see the Best Practices Guide for High-Density Design and Deployment.

VPN Provisioning

Initial VPN provisioning requires that the APs be placed in the same Layer 2 subnet as the controller. The controller VPN server must be started, and the APs that have certificates installed are added to the VPN group. (Not all Meru AP models support VPN functionality.) The APs then establish the VPN tunnel to the controller after a reboot. After confirming the VPN status, each AP can be disconnected from the local network and is ready to deploy in any geographic location.

APs can perform normal Layer 2 and Layer 3 discovery of controllers in addition to VPN. However, if a VPN-enabled AP fails to establish a connection to the controller, the AP can switch back only to L2 mode.

For information about configuring VPN, see the *Meru System Director Configuration Guide* on the Customer Support Portal.

Certificates

Digital certificates are exchanged between controllers and APs during the handshake process before establishing a VPN connection. To use VPN, you can use the default AP and controller certificates or certificates signed by third-party CAs can be used for VPN. Table 2 explains the actions to be taken considering different combination of certificates, a scenario if the certificate is lost or corrupted, or if the VPN certificate has to be changed.

Table 2: AP-Controller Certificate Matrix

AP	Controller	Action
Default certificate	Default certificate or third-party certificate	Add the APs to VPN group.
No certificate*	Default certificate	Obtain the AP certificate from Meru Support.
No certificate	Third-party certificate**	Obtain the AP certificate from Meru Support. For third-party certificates, generate the CSR and get it signed from the CA, and upload to the controller.
NA	While changing the certificate in controller used by VPN	Upload the certificates to controller and use the Download CA button*** to copy the CA to all APs.

* The AP110 and AP1014i are shipped with factory-installed certificates. If an AP certificate is accidently deleted or is not working as expected, a new certificate must be obtained.

** If you are already using third-party certificates for Captive Portal or Web UI, you can also use those certificates for VPN.

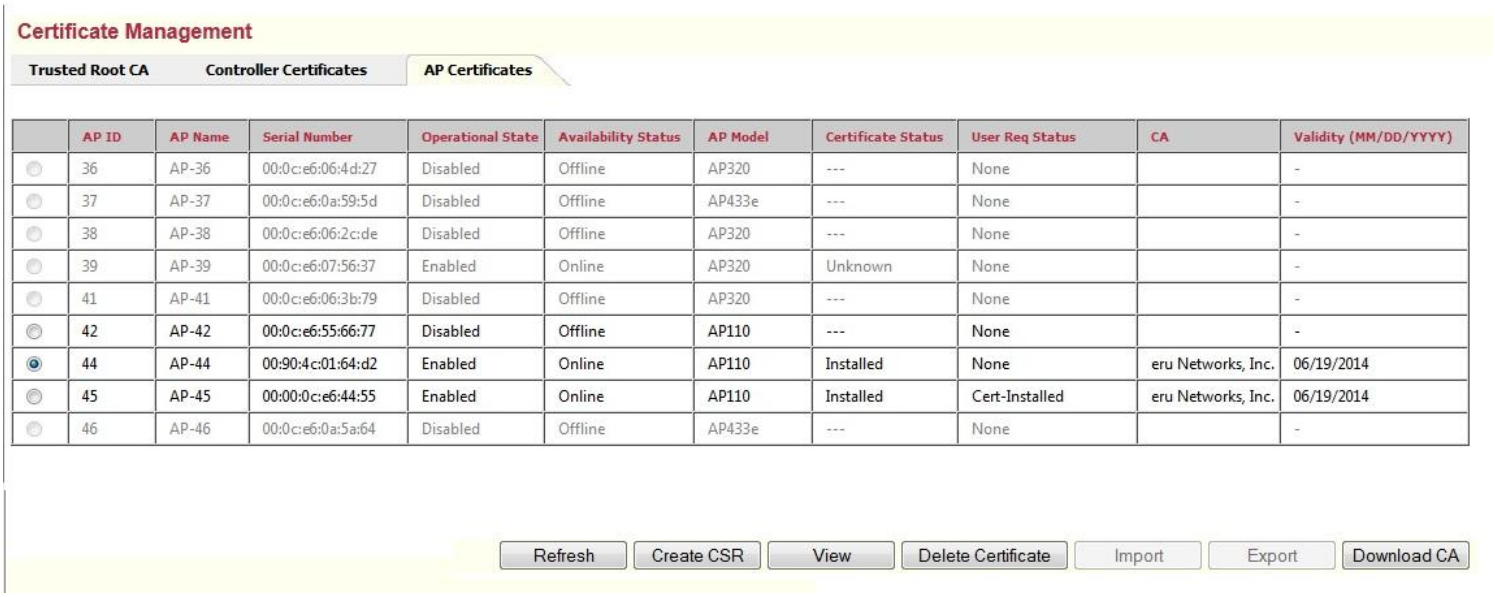
*** Use the Download CA button to change the certificate used by VPN. Before changing the certificate, it is important to copy the new certificate's CA to the APs; otherwise, the VPN connectivity will be broken. After uploading the new certificates to the controller, download the CA to the APs by using the Download CA button. A copy of the controller CA is pushed to each AP, and the APs will trust the controller certificates the next time it negotiates the VPN connection. After the CA is pushed to each AP and the VPN certificate is changed, issue the `reload-vpn` command from the controller CLI.

To download the controller CA for APs:

1. Select **Configuration > Certificates**.
2. Select the **AP Certificates** tab. The AP Certificate page appears, as shown in Figure 2.
3. Select each AP for which to download the controller CA.
4. Click **Download CA**.

After VPN certificate is changed, issue the `reload-vpn` command from the controller CLI.

Figure 2: AP Certificate Page



	AP ID	AP Name	Serial Number	Operational State	Availability Status	AP Model	Certificate Status	User Req Status	CA	Validity (MM/DD/YYYY)
○	36	AP-36	00:0c:e6:06:4d:27	Disabled	Offline	AP320	---	None		-
○	37	AP-37	00:0c:e6:0a:59:5d	Disabled	Offline	AP433e	---	None		-
○	38	AP-38	00:0c:e6:06:2c:de	Disabled	Offline	AP320	---	None		-
○	39	AP-39	00:0c:e6:07:56:37	Enabled	Online	AP320	Unknown	None		-
○	41	AP-41	00:0c:e6:06:3b:79	Disabled	Offline	AP320	---	None		-
○	42	AP-42	00:0c:e6:55:66:77	Disabled	Offline	AP110	---	None		-
◉	44	AP-44	00:90:4c:01:64:d2	Enabled	Online	AP110	Installed	None	eru Networks, Inc.	06/19/2014
○	45	AP-45	00:00:0c:e6:44:55	Enabled	Online	AP110	Installed	Cert-Installed	eru Networks, Inc.	06/19/2014
○	46	AP-46	00:0c:e6:0a:5a:64	Disabled	Offline	AP433e	---	None		-

Wireless (ESS) Profiles

The AP110 and AP1014i support tunneled and bridged modes for wireless (ESS) profiles. The AP110 supports a maximum of 10 wireless stations.

Wired Port Profiles

The AP110 and AP1014i support tunneled and bridged modes for wired port profiles.

AP wired interfaces that are part of a port profile share the same configuration. The traffic from the wired stations connected to the AP interfaces that are part of the port profile can be tunneled back to the controller or locally bridged. Multiple port profiles can be created with different configurations for different sets of APs.

Keep the following in mind when an AP is part of a port profile that supports wired stations:

- When a secondary Ethernet port is bound to the Meru tunnel, the AP tunnels all packets between the devices attached to that port and the controller. In tunnel mode, traffic always goes to the controller and then gets forwarded to the destination.
- The interfaces can be in different modes (for example, the wired interface can be bridged, whereas wireless can be tunneled and vice versa).
- Each device connected to an additional Ethernet port is visible as a wired station on the AP for management and monitoring purposes. The `show station wired` CLI command displays wired stations.
- If the wired interface data plane is in tunnel mode and the device is a VoIP phone that uses SIP, it will be visible as a SIP phone on the controller's phone database. The `show phones` CLI command lists wired phones.

- IPv6 bridging is supported for wired stations, just as it is for wireless stations.
- Wired station assignment is also managed by the controller. The controller communication includes connect, assign, and delete messages between the AP and controller for a wired station assignment and removal from station database.
- The age out timer for wired stations is 1800 seconds (30 minutes). In other words, a wired station that is idle for 1800 seconds is automatically removed from the station table.

You can enable the default wired port profile using the Web UI or CLI.

Web UI

To enable the default wired port profile:

1. Select **Configuration > Wired > Port**.
2. Select the check box for the default profile, and click **Settings**.

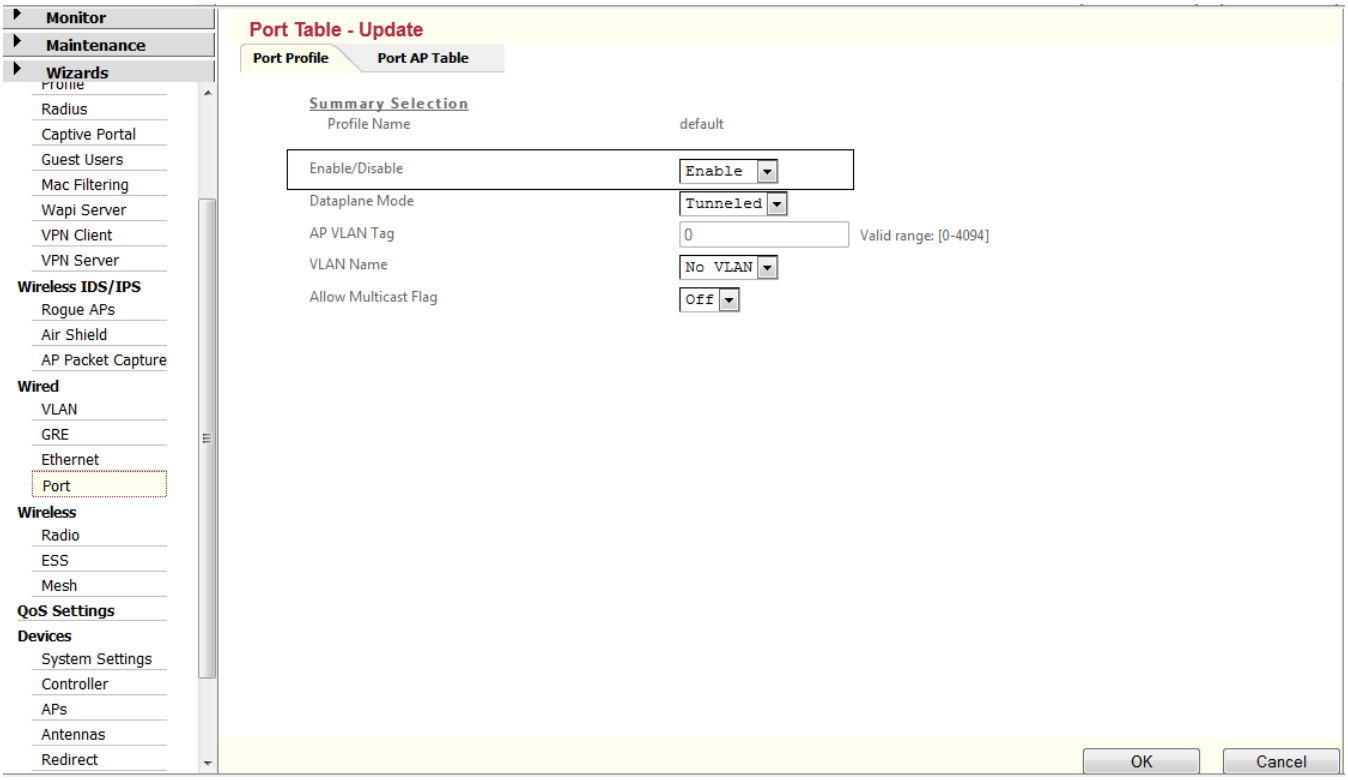
   The Port Table page appears, as shown in Figure 3. The VLAN, Dataplane Mode, and Multicast settings are applicable only for the APs that are part of this profile.
3. In the Enable/Disable list, select **Enable**.
4. Click **OK**.

CLI

To enable the default wired port profile, use the following commands. For the last command, substitute the AP ID value for *ap-id*.

```
controller(config)# port-profile default
controller(config-port-profile)# enable
controller(config-port-profile)# port-ap ap-id
```

Figure 3: Default Port Table Page

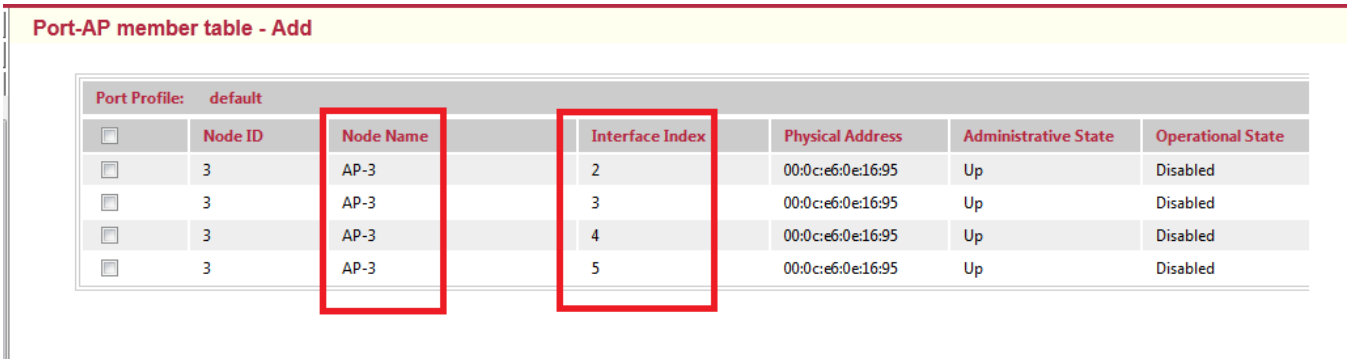


To add AP interfaces to the default port profile:

1. Select **Configuration > Wired > Port**.
2. Select the check box for the default profile, and click **Settings**.
3. Click the **Port AP Table** tab.

   The Port-AP Member Table page appears, as shown in Figure 4. In this example, there are multiple interfaces listed because the AP is an AP1014i.
4. Click **Add**.
5. Select the check boxes of the AP interfaces.
6. Click **OK** to add the AP interfaces to the port profile.

Figure 4: Port-AP Member Table Page (AP1014i)



Differences Between AP110 and AP1014i Wired Interfaces

There are two ports labeled as F1 and F2 on the AP110. F1 is the LAN port and is yellow. F2 is the WAN port and is green. On the AP1014i, the LAN ports are yellow, and the WAN port is green. The rear view of the AP110 is shown in Figure 5. The rear view of the AP1014i is shown in Figure 6.

Figure 5: AP110 Rear View

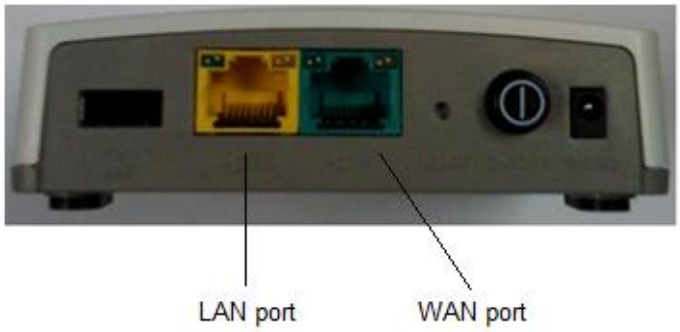
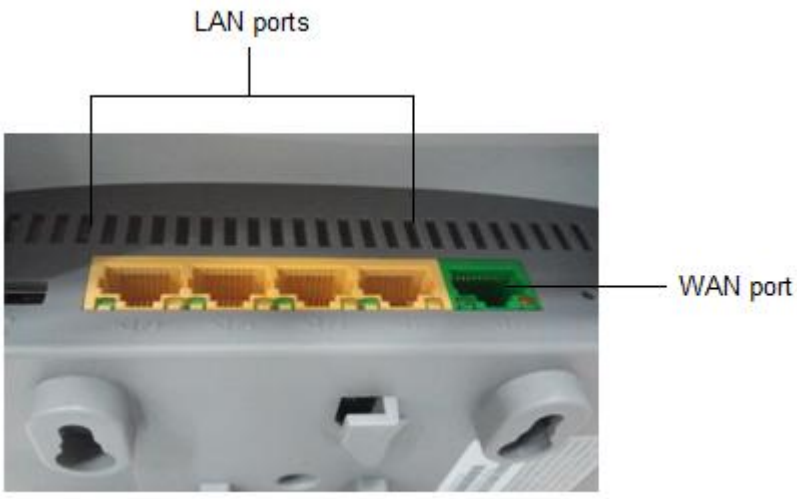
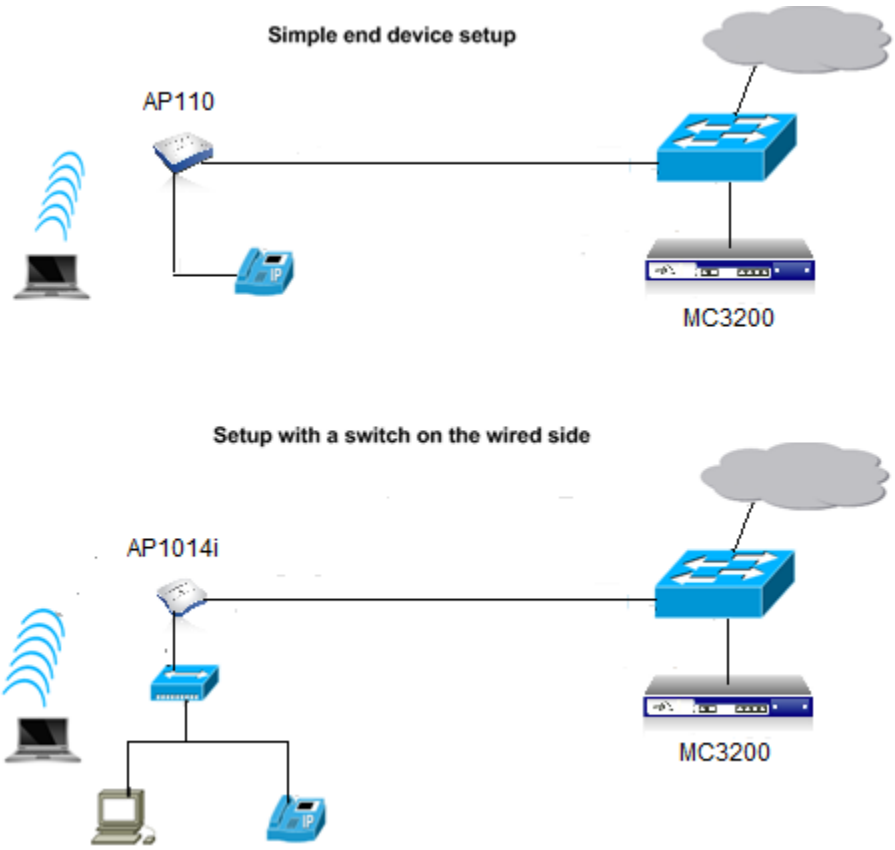


Figure 6: AP1014i Rear View



The configuration takes effect on those APs that are part of a port profile. Multiple port profiles can be configured on the controller with different configurations for different APs.

Figure 7: AP110 and AP1014i Deployment with Wired Device Support



VLANs

VLANs are supported in tunnel mode for wired and wireless profiles. The traffic from the client is always untagged, and the controller maps the traffic to the correct VLAN. Multicast traffic can be optionally filtered.

VLANs are not supported in bridge profiles (wired and wireless).

The multiple interfaces of an AP1014i are all members of the same VLAN.

Table 3 lists the VLAN tagging support for Meru access points. For Meru APs with additional Ethernet ports, VLAN tags are not added to outgoing packets destined for wired clients on those Ethernet ports.

Table 3: VLAN Tagging Support

Profile Type	AP110	AP1014i	AP1010	AP1020	AP320	AP332	AP433
Wireless profile (tunneled)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Wireless profile (bridged)	No	No	Yes	Yes	Yes	Yes	Yes
Port profile (tunneled)	Yes	Yes	NA	NA	NA	Yes	NA
Port profile (bridged)	No	No	NA	NA	NA	No	NA

Mesh

The AP110 and AP1014i are single-radio, 2.4GHz-only devices and can only be leaf nodes in a mesh cloud. Additionally, this means that clients and backhaul share the bandwidth.

The following provides some general information about a Meru mesh network implementation:

- Wireless backhaul link: A wireless connection over which an AP is connected to a controller. Backhaul links are encrypted on a per-hop basis using WPA2-PSK.
- Hop: A hop is when a connection passes over a wireless backhaul link. The mesh network supports a maximum of three (wireless) hops.
- Node: An AP participating in a mesh network.

  Any given node cannot be part of multiple mesh clouds. The maximum number of nodes supported in a mesh cloud is 16, and the maximum number of stations is 500.

  All nodes behind a wireless backhaul can only be connected to the same controller as the gateway AP.
- Mesh cloud: A group of mesh APs that can connect to each other to form a mesh. Only nodes that are in the same mesh cloud are able to establish mesh connections.

  Each mesh cloud has one pre-shared key (PSK). When a node comes online, it automatically downloads and installs the PSK.
- Virtual Cell and QoS parameters are supported over mesh links.

AP Roles

APs can operate in different roles in a mesh network, depending on their location in the network. APs can be in one of the following roles in a network.

Access Nodes

An access node is an AP that does not have any wireless backhaul connection (in other words, an AP that is not participating in the mesh setup).

Gateway Nodes

A gateway node is an AP that uses a wired backhaul connection to the controller and can support wireless backhaul connections from other nodes

Gateway nodes use beacons to advertise their backhaul capability over the air.

Mesh and Leaf Nodes

A mesh node is an AP that uses a wireless backhaul connection to the controller and can support wireless backhaul connections from other nodes.

A leaf node is an AP that uses a wireless backhaul to connect to the controller but does not support wireless backhaul from any other nodes.

The AP110 and AP1014i have built-in mesh capability but can be configured only as leaf APs in the mesh cloud. This means that the APs have to be added to a mesh profile to enable the mesh services. (Enabling mesh services on wireless interfaces allows an AP to do backhaul.)

Mesh and leaf nodes use beacons to advertise their backhaul capability over the air.

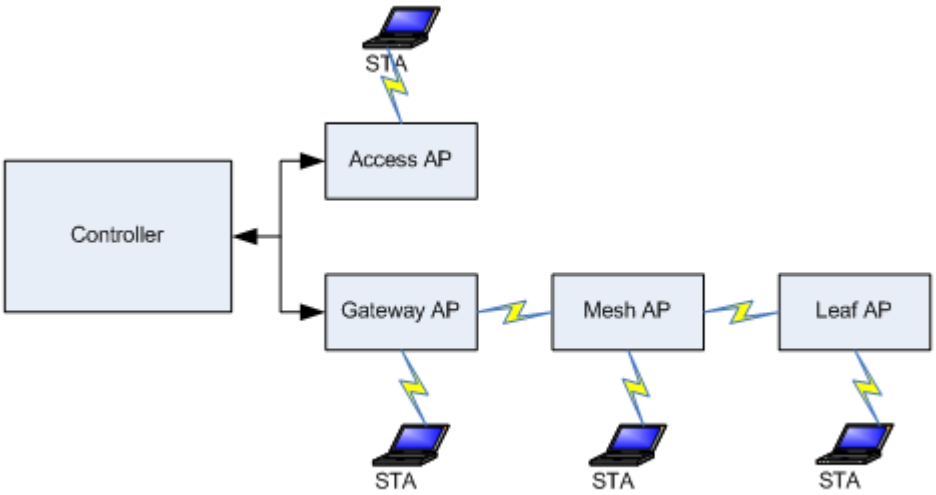
Mesh and leaf nodes provide only tunneled access. Bridged mode is currently not supported in a mesh environment. Mesh and leaf nodes cannot be part of ESS profiles configured for bridged mode.

Mesh and leaf APs automatically discover the best uplink node to connect to. The RSSI of the parent node is used as the primary gauge. If the RSSI values of multiple parent nodes are similar; the number of hops is used as the tiebreaker.

A mesh node monitors the uplink connection. In case of a link failure, if there is another parent node available, the mesh node automatically switches to the new parent node without losing connectivity to the controller and the stations associated to it.

The unused Ethernet port on a mesh node (mesh/leaf) can be used in a manner similar to an Ethernet switch port. Users can plug their devices into this port and gain access to the network.

Figure 8: Different Mesh Nodes



	Requires Wireless Backhaul	Provides Wireless Backhaul
Access AP	No	No
Gateway AP	No	Yes
Mesh AP	Yes	Yes
Leaf AP	Yes	No

In a mesh network, nodes have a parent/child relationship. How a node is identified depends on the relative position of the nodes in a mesh tree. For any two nodes with a mesh connection, the node closest to the gateway is the parent, and the other node is the child.

An uplink is the wireless connection to the parent AP (from the perspective of a mesh node). A downlink is the wireless connection (or set of connections) toward child mesh APs/nodes (from the perspective of a mesh node).

Characteristics of a Wireless Backhaul Connection

Nodes using a wireless backhaul connection can connect to the controller only using Layer 3. One controller can support multiple gateway nodes.

An uplink connection is always established using the highest numbered radio (radio1) on the AP. The downlink connection can be offered on any radio. The radio being used to provide wireless backhaul can also be used to provide service/access to clients. A node can provide downlink service on the same or different radio than the one being used to provide uplink service. For the AP110 and AP1014, client access and backhaul share the radio.

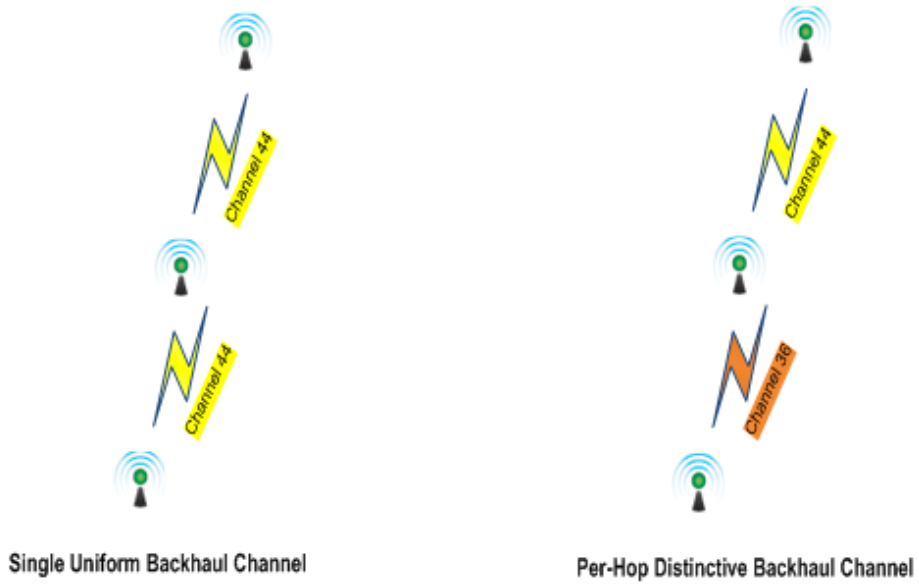
Although the backhaul uplink is always provided by the highest numbered radio on the AP, the channel usage on that radio can vary between two (or more) backhaul nodes, as shown in Figure 9.

There are no restrictions on the frequency band, channel, or channel-width for the radio being used for backhaul. For nodes that require wireless backhaul, channel parameters are inherited from the parent AP and are not configured independently on the child AP.

A radio that is participating in the mesh service will not change channels and only performs rogue detection/mitigation on the home channel.

When using a Per-Hop Distinctive Backhaul channel (shown in Figure 9), the second radio of the parent AP is used to exchange mesh information with the downlink radio (which itself might be the first or second radio of the child AP).

Figure 9: Backhaul Channel Establishment



For an example of a mesh implementation with the AP110 and AP1014i, see Use Case 5 Design Example: Leaf AP in a Mesh Cloud.

Design Examples

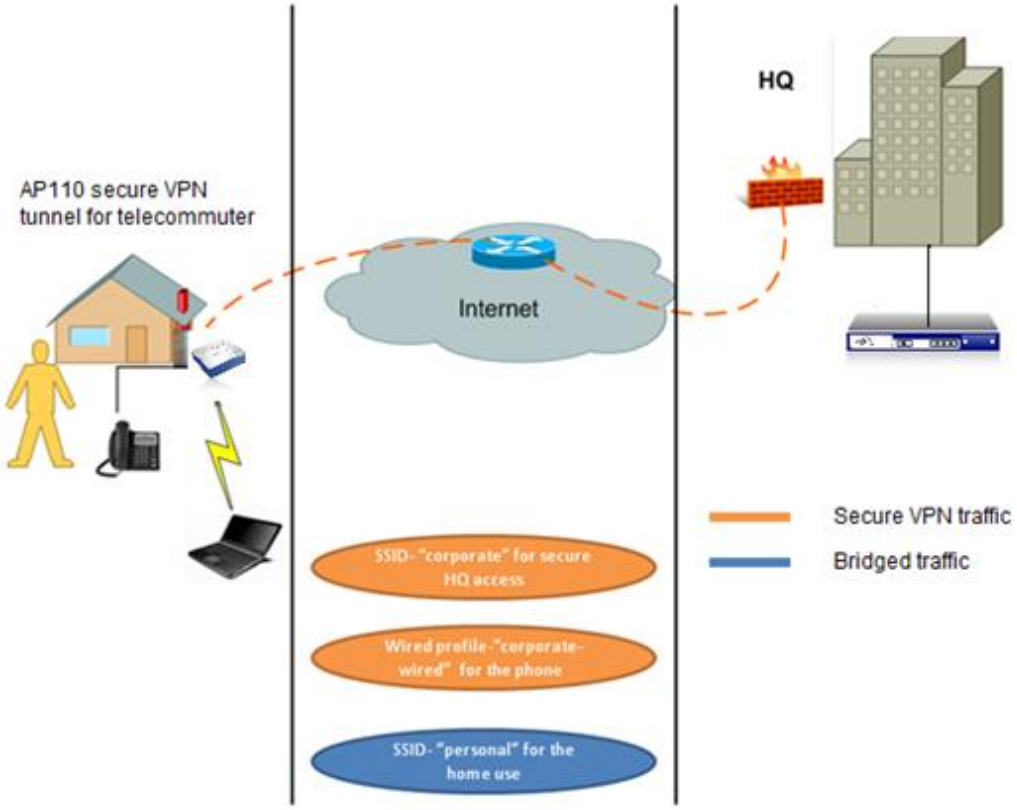
The following use cases illustrate examples of AP110 and AP1014i deployments:

- Use Case 1 Design Example: Using the AP110 as a Telecommuter AP for the Home Office
- Use Case 2 Design Example: Using the AP1014i as a Telecommuter AP for the Home Office
- Use Case 3 Design Example: Branch Office Deployments
- Use Case 4 Design Example: In-Room AP for Wireless and Wired Service
- Use Case 5 Design Example: Leaf AP in a Mesh Cloud

Use Case 1 Design Example: Using the AP110 as a Telecommuter AP for the Home Office

A telecommuter in a home office requires secure access to corporate resources using a simple and inexpensive VPN infrastructure from the home office. Personal use of wireless must also be provisioned, which cannot impact corporate network access. A wired phone in the home office using a corporate extension should integrate seamlessly with the corporate infrastructure. Figure 10 illustrates the use case scenario.

Figure 10: Telecommuter AP



With built-in VPN capability, the AP110 allows a user to connect to and access the corporate resources (wired and wireless) through a secure tunnel. The traffic from the phone connected to the wired interface of the AP is tunneled back to the controller. Family members can use the AP110 to access the Internet using a personal SSID configured in bridge mode.

Before giving an AP110 to a telecommuter, you must provision the AP110 for VPN. For information about initial VPN provisioning, see VPN Provisioning.

If the user loses the AP110 or leaves the organization without returning the AP, deprovision the AP so that unauthorized users cannot access your network:

- Remove the AP110 from the VPN group.
- Remove the relevant ESS-AP entries.
- Remove the relevant Port-AP table entries.

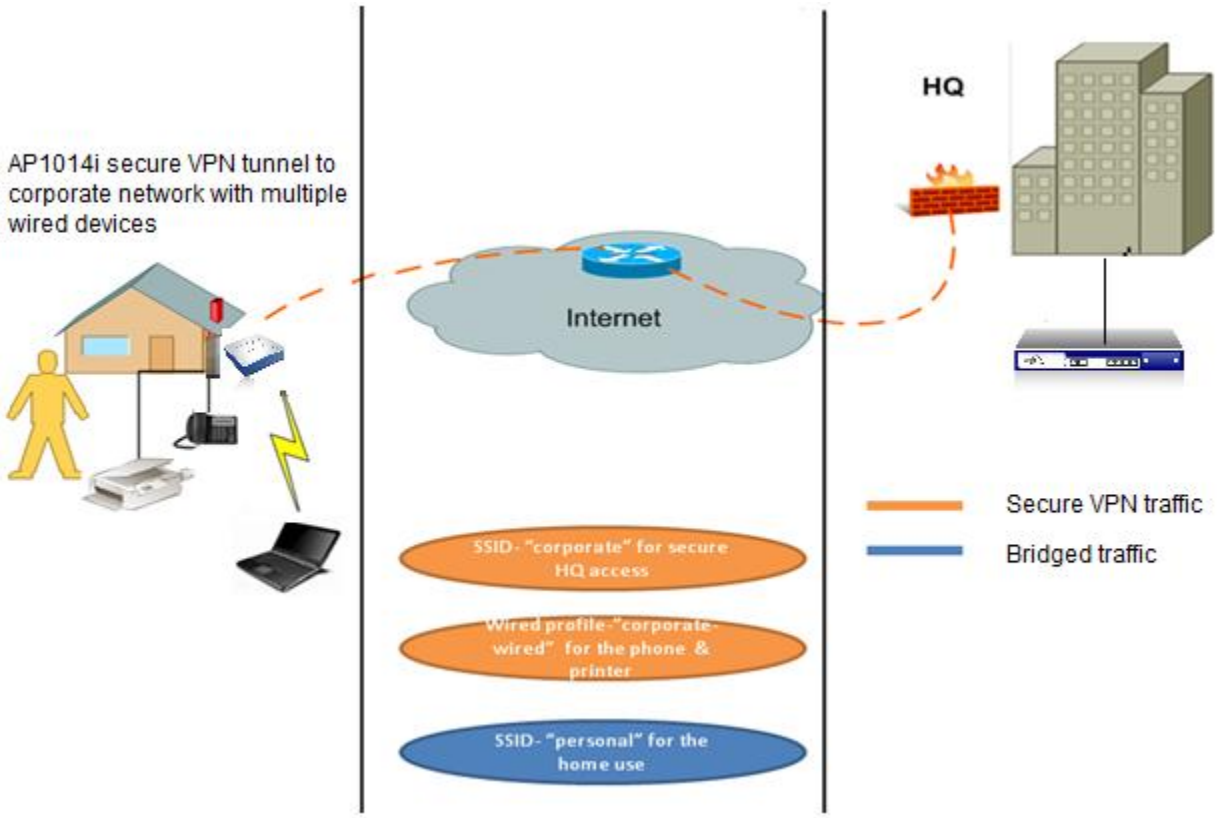
The following is configured for this use case:

- A tunneled ESSID named “corporate” is created for corporate network access. Corporate user security is applied to this ESSID.
- The AP wired interface is part of the port profile named “corporate-wired,” which is in tunneled mode to the controller. The phone is connected to this AP interface.
- A bridged ESSID named “personal” is created for home use. The traffic in this ESSID is passed to the Internet locally. The security used is WPA2-PSK.

Use Case 2 Design Example: Using the AP1014i as a Telecommuter AP for the Home Office

The requirements are almost the same as in Use Case 1. However, this use case requires that multiple wired devices be associated to the same AP (for example, a printer in addition to the phone). An employee must be able to easily send print jobs, while accessing email and other corporate resources like file servers, without switching between SSIDs to connect to a local printer. The bridged SSID for personal access to the Internet is also applicable for this use case. Figure 11 illustrates the use case example.

Figure 11: Telecommuter AP with Multiple Wired Device Support



With the AP1014i, the four additional Ethernet ports allow the telecommuter to attach additional wired devices. The corporate network is accessed through a secure VPN tunnel. A phone with a corporate extension and a printer also can be connected to the wired interfaces of the AP. A user connected to the corporate SSID can send print jobs easily and also use the phone with a corporate extension. Family members at home can access the Internet using the bridged SSID of the same AP.

Before giving an AP110 to a telecommuter, you must provision the AP110 for VPN. For information about initial VPN provisioning, see VPN Provisioning.

If the user loses the AP110 or leaves the organization without returning the AP, deprovision the AP so that unauthorized users cannot access your network:

- Remove the AP110 from the VPN group.
- Remove the relevant ESS-AP entries.
- Remove the relevant Port-AP table entries.

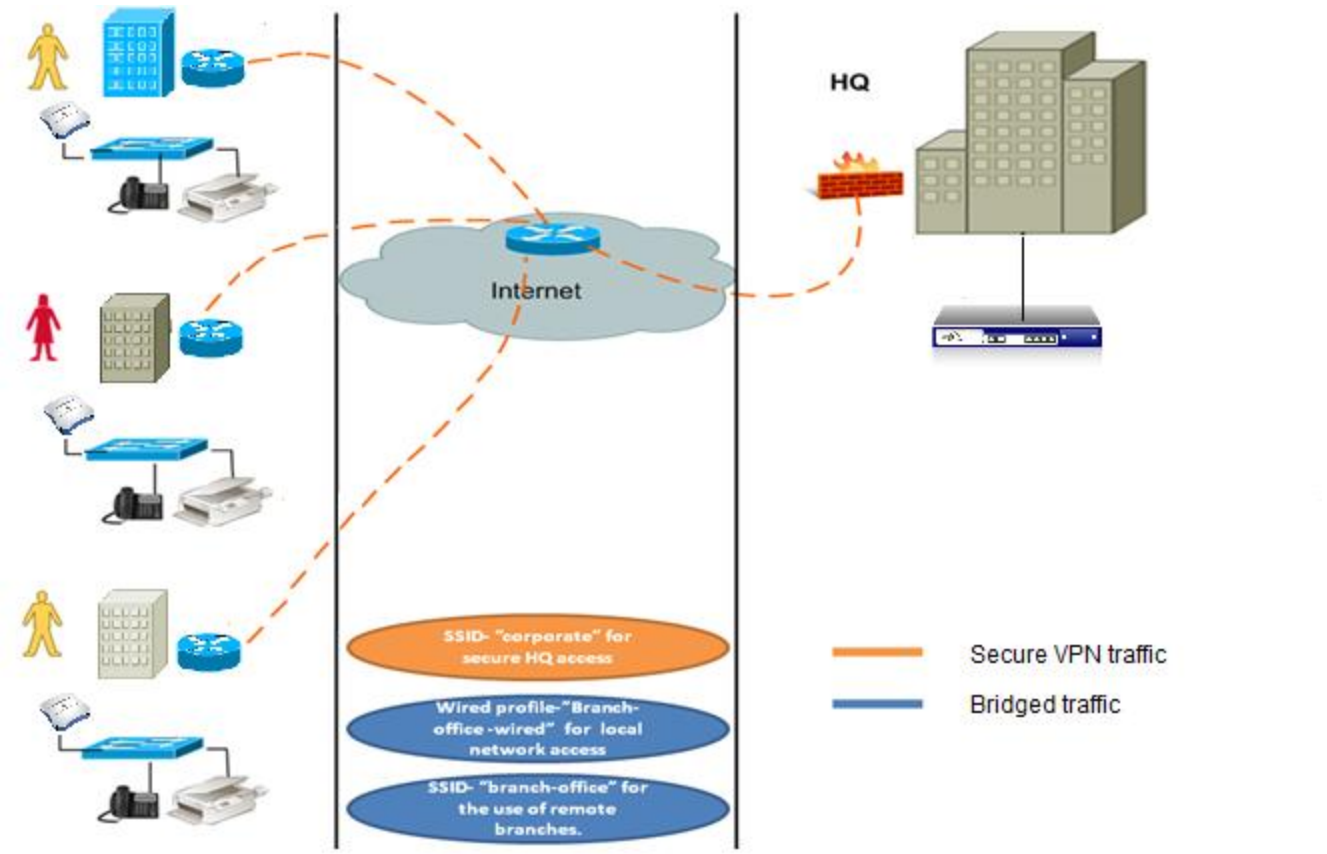
The following is configured for this use case:

- A tunneled ESSID named “corporate” is created for corporate network access. Corporate user security is applied to this ESSID.
- The AP wired interfaces are part of a port profile named “corporate-wired,” which is in tunneled mode. The phone and printer are connected to these AP interfaces.
- A bridged ESSID named “personal” is created for home use. The traffic in this ESSID is passed to the Internet locally. The security used is WPA2-PSK.

Use Case 3 Design Example: Branch Office Deployments

Branch offices do not need frequent access to Headquarters, but they should be able to share local network resources using a cost-effective solution. One or more APs are deployed, which support wired and wireless access. A network switch is connected to the AP interface to support additional wired stations. An SSID with corporate network access is also required for visiting corporate users to allow them to connect to Headquarters. The traffic between corporate and branch offices must be secure. A large office having branches throughout the city is a typical example and is shown in Figure 12.

Figure 12: AP1014i Branch Office Deployment



After VPN-enabled APs that are deployed in branch offices, which are geographically dispersed, are connected to the Internet, the APs automatically establish a tunnel with the Headquarters network.

The APs are still managed by the centralized controller, which also performs configuration tasks, real-time statistics gathering, troubleshooting, and so on. For this particular deployment scenario, a tunneled SSID is made available in all branch offices for visiting HQ users. The branch office users will be connecting to a bridged SSID/wired port profile for the branch users to share local network resources.

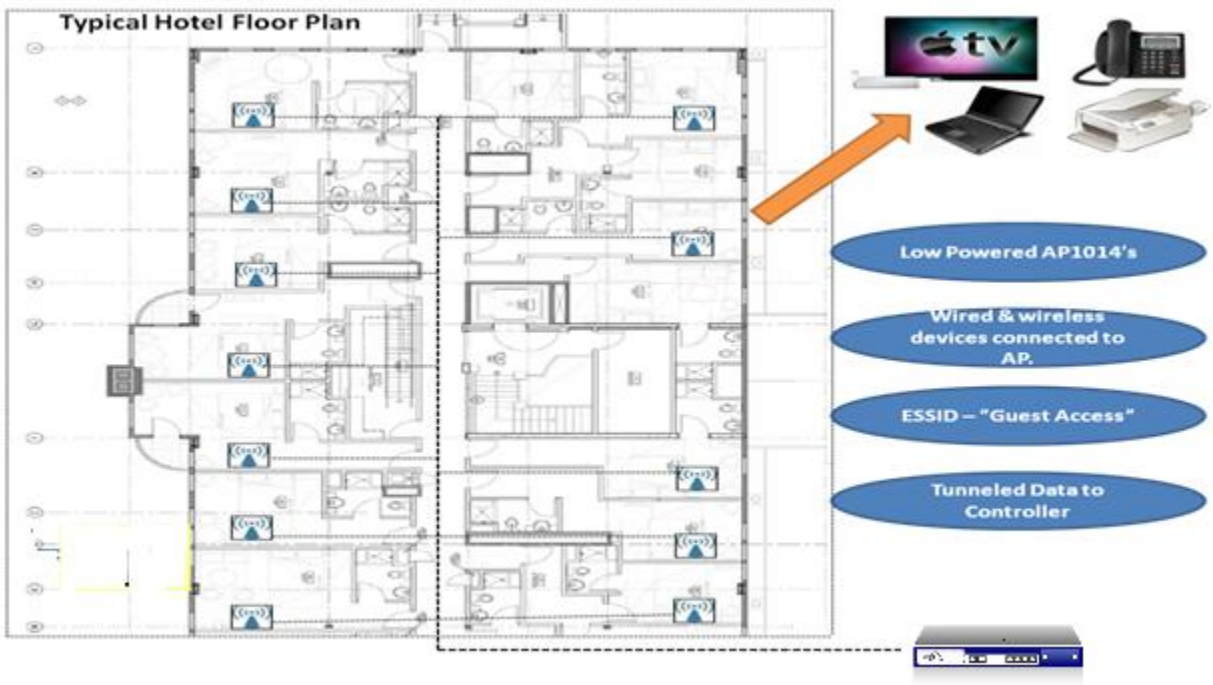
The following is configured for this use case:

- A tunneled ESSID named “corporate” is created for corporate network access. Corporate user security is applied to this ESSID.
- The AP wired interfaces are part of a port profile named “Branch-office-wired,” which is in bridged mode. All traffic originated from devices directly connected to the wired interfaces of the AP or from the network switch is forwarded to the local network.
- A bridged ESSID named “branch-office” is created for branch-office use. The traffic from users connected to this ESSID is also forwarded only in the local network. Wired and wireless users can also share local network resources at the same time.

Use Case 4 Design Example: In-Room AP for Wireless and Wired Service

The hospitality industry is seeing a rise in guests’ smartphones usage, but there are many hotels still providing only wired Internet service in guest rooms. In a situation where guests need to use smartphones or tablets to access the Internet in hotel rooms using Wi-Fi, there is a need to deploy access points. Traditional access points are placed in hallways or common outlets, which sacrifices the coverage and throughput requirements. Providing in-room access becomes a huge administrative effort with tedious channel planning and costly site surveys, and pulling new wiring can also destroy the interior decoration. Providing IPTV, IP phones, and printers as guest services in hotels adds to the complexity of adding additional cable drops to rooms. Figure 13 illustrates this use case.

Figure 13: In-Room Tunneled AP



The AP1014i solution minimizes the Wi-Fi deployment cost, as you can reuse the existing network infrastructure and replace only the wired Internet socket; this allows rapid deployment in every room. The cost-saving solution does not need to pull new wirings for Wi-Fi Internet installation. Hotels that want to install IPTVs, IP phones, and so on can use the additional Ethernet ports available in the AP and can also be segregated from the wireless traffic by using VLAN segmentation. The AP1014i fully supports Meru Virtualization, so the APs can remain in a single channel, which avoids costly site surveys and channel conflicts while trying to achieve the desired wireless coverage in every room.

The following is configured for this use case:

- APs deployed in each room are in Layer 2 or Layer 3 mode, which is optional.
- The APs are connected to the PoE-enabled single cable drops in each room.
- The wired interfaces of the APs can be connected to an IPTV, IP phone, printer, and so on.
- The ESSID named “guest-access” is configured for Wi-Fi, which is common across the hotel.
- An AP deployed in each room can result in a high AP density network, which might cause high RF noise levels. These high noise levels might affect performance. To optimize performance, check the RF noise levels and adjust power as necessary.

Use Case 5 Design Example: Leaf AP in a Mesh Cloud

Some hotel infrastructures prevent installing an Ethernet drop in each room; the available Ethernet drops might be limited for each floor. The alternate Wi-Fi solution might not be reliable and pervasive across the property. In outdoor hospitality venues within the same premises, it is difficult to extend the wiring for an access point in areas like pools, open lawns, and so on. Many hotels, convention centers, resorts, and cruise ships are choosing mesh nodes that can quickly and easily create a wireless mesh network, eliminating the need for a traditional wired Ethernet backhaul. The mesh network use case is also applicable in any scenarios where expected client density is low and no bandwidth-intensive applications need to be run over the wireless network.

Figure 14 illustrates a hotel floor in which there are rooms that have no cable drops to provide Internet connections. By providing an in-room AP with mesh backhaul, the wireless coverage is extended, and additional wired devices can also be attached.

Figure 14: In-Room Mesh AP

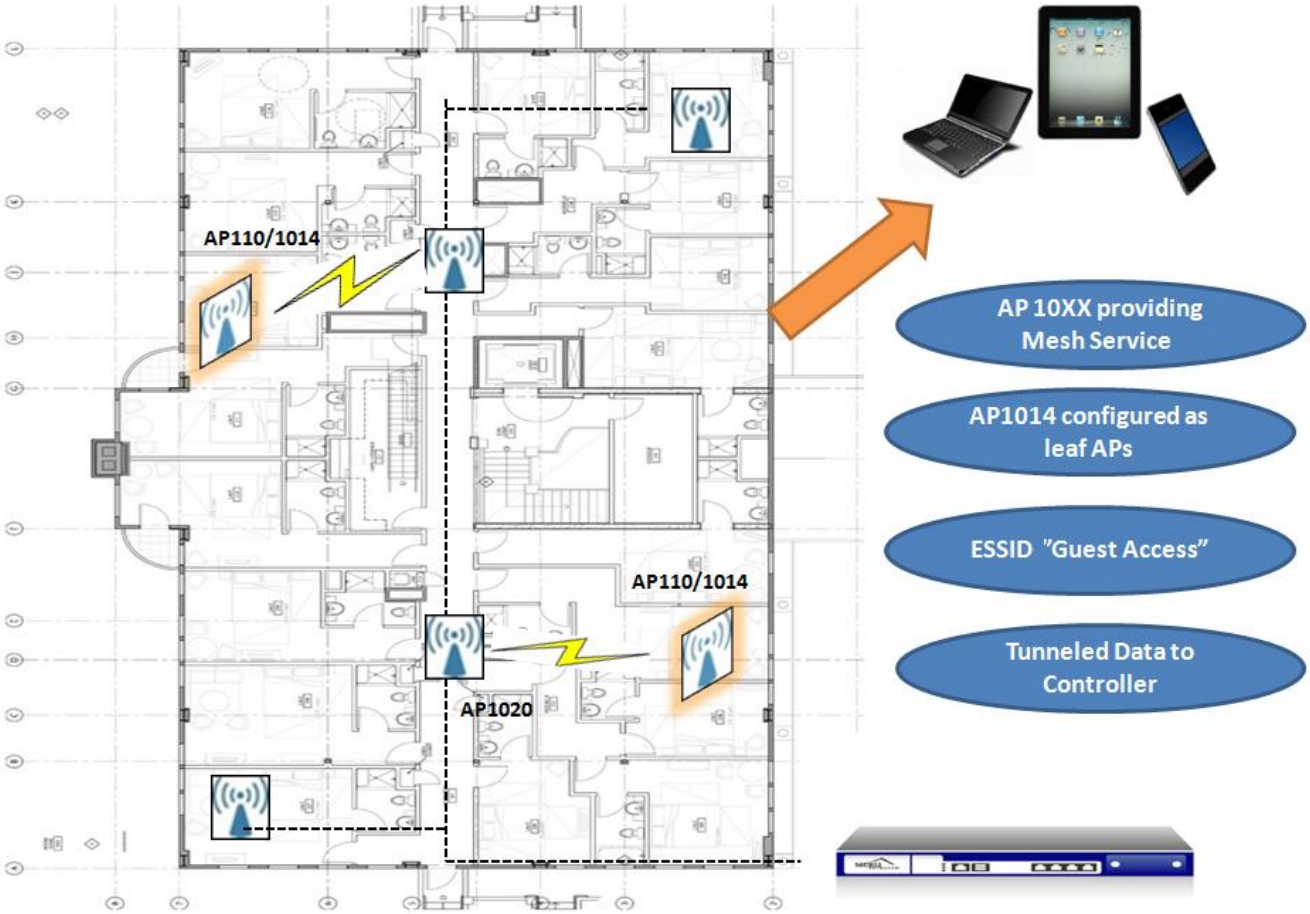


Figure 15 shows the solution for another hotel scenario in which coverage needs to be extended to the outdoor areas. Multiple mesh or gateway APs provide seamless connectivity for APs configured in leaf mode. As shown in the diagram, there are AP1010/1020 access points configured in tunneled mode that communicate to the controller, which also provides wireless backhaul. The AP110 or AP1014i access points that are deployed outside join the mesh cloud, advertising the wireless service in respective areas.

Figure 15: Extending Limited Outdoor Coverage Using Mesh

The AP110 and AP1014i support mesh, which allows repeating the signal of other access points, eliminating the need to run Ethernet cabling to each AP. Mesh makes it easy to provide enhanced coverage to hard-to-reach areas by plugging in an AP to power using a PoE injector. Meru mesh works out of the box with zero configuration, making it easy to plug in repeaters in areas where there are no convenient Ethernet ports. With Meru Virtualization, there is no channel planning needed; wherever there is a coverage gap, an AP can be deployed.

The following is configured for this use case:

- A mesh license is installed on the controller.
- Gateway or mesh APs must be identified and configured before deploying the AP1014i.
- Design a “mesh cloud” in the controller with two or more gateway/mesh APs so that there are multiple backhaul links to support failover.
- Configure the AP110 and AP1014i as leaf APs in a mesh cloud. If the APs have to be placed outdoors, proper enclosures must be used. A PoE injector should be available to use in conjunction with a power source.
- After the AP goes online with the controller, extend the ESSID named “Guest Access” to provide wireless service in the area.

Implementation Guidelines

Consider the following when implementing your WLAN:

- AP Mounting
- Antenna Radiation Patterns

AP Mounting

The AP110 is designed to be mounted on a horizontal flat surface (such as a desktop or table) or a vertical surface (such as a wall). The radios provide 360° of coverage. For powering up, a 12 V DC adapter is supplied with the AP. The AP1014i, just like the AP1010 and AP1020 models, can be wall mounted or ceiling mounted.

For more information, see the AP installation guides on the Meru Customer Support Portal.

Antenna Radiation Patterns

The AP110 and AP1014i have omni-directional antennas providing 360° coverage. The peak antenna gain is 2 dBi. Figure 16 and Figure 17 show the radiation patterns for the AP1014i. Figure 18 and Figure 19 show the radiation patterns for the AP110.

Figure 16: AP1014i X-Y Plane Radiation Pattern

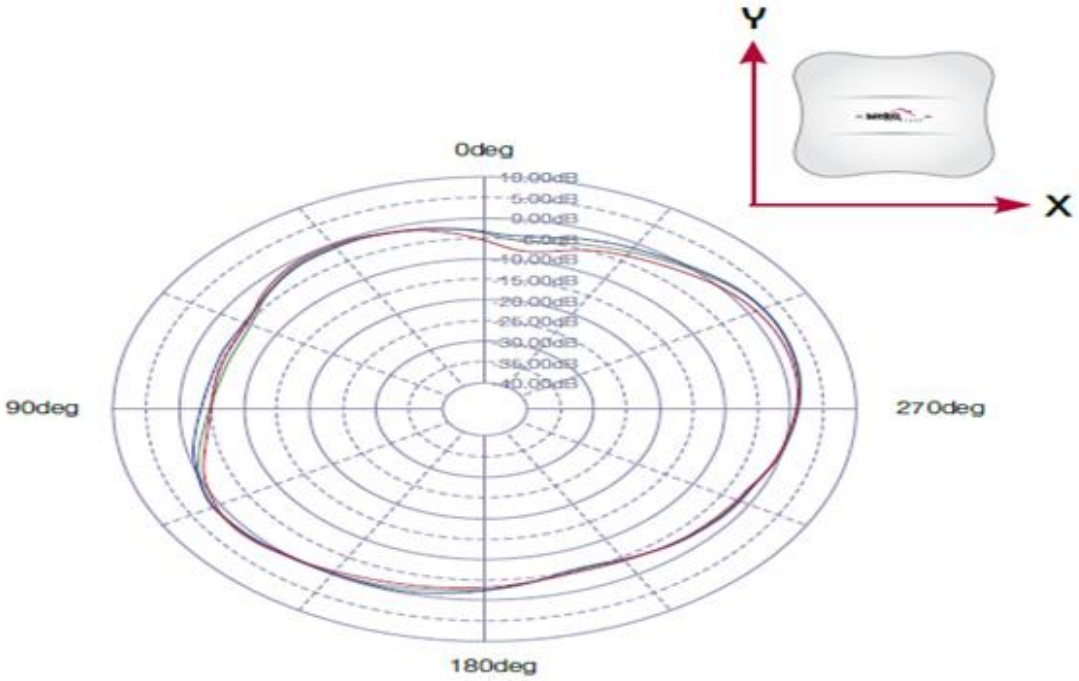


Figure 17: AP1014i X-Z Plane Radiation Pattern

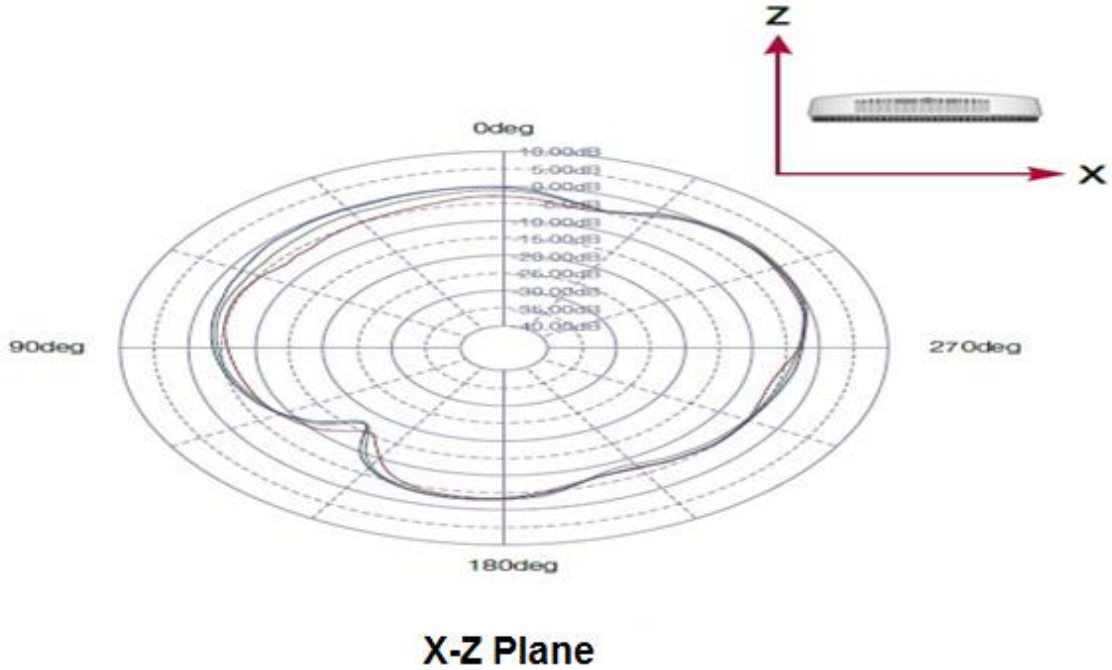
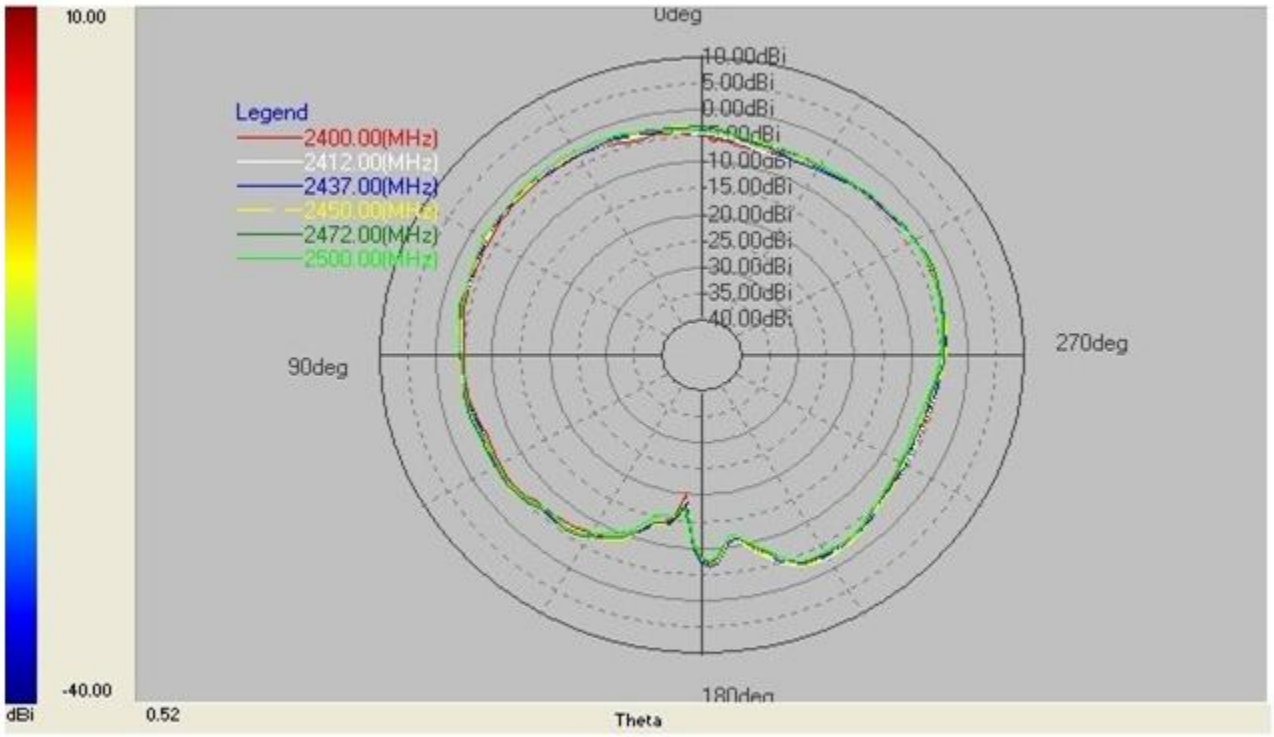
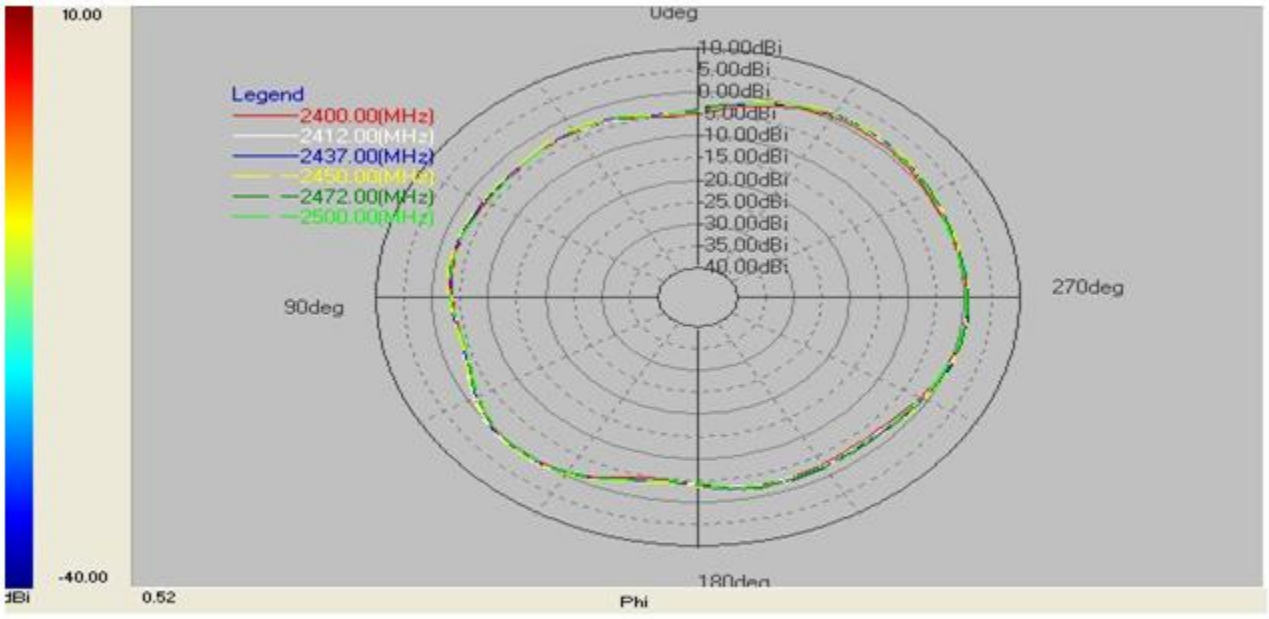


Figure 18: AP110 X-Y Plane Radiation Pattern



X-Y Plane

Figure 19: AP110 X-Z Plane Radiation Pattern



X-Z Plane

For more information, see the AP installation guide on the Customer Support Portal.

AP110 and AP1014i Monitoring and Management Commands

You can use the CLI to monitor and manage VPN and the mesh network.

VPN

To display the VPN server status and VPN IP pool, use the following command:

```
controller# show vpn-server
```

To display a list of VPN-connected APs, use the following command:

```
controller# show vpn-ap
```

To display the VPN status of an AP, use the following command:

```
controller# show ap-connectivity ap-id
```

Substitute the AP ID value for *ap-id*.

To display VPN status, use the following commands:

```
controller# conn ap ap-id
```

Substitute the AP ID value for *ap-id*.

```
ap id> ip vpn show

VPN  Status          : Enabled
VPN Server Host Name :
Controller Public IP : 172.18.41.16
Controller Tunnel IP : 192.168.2.1
Controller VPN Port  : 1194
Data Encryption      : Enabled
VPN Connect Mode     : Enabled
ap 3>
```

If any changes are made in certificates used for VPN, use the following command:

```
controller(config)# reload-vpn
```

Use the following commands to add or remove an AP from a VPN group:

```
controller(config)# ap ap-id
controller(config-ap)# connectivity l3-preferred
controller(config-ap-connectivity)# vpn
controller(config-ap-connectivity)# no vpn
```

To display certificate and CA information and the connectivity mode of an AP:

```
controller# show ap-certificate ap-id
```

Mesh Network

To display the mesh status for APs, use the following command:

```
controller# show mesh-ap
```

To display the configured mesh profile on the controller, use the following command:

```
controller# show mesh-profile
```

Detailed output of each command is provided in the *Meru System Director Command Reference Guide*, available from the Customer Support Portal.

Where to Find More Information

- AP110 Installation Guide
- AP1014i Installation Guide
- Meru System Director Configuration Guide and Meru System Director Command Reference (On the Software Downloads & Documentation page, click the link for the release of System Director that you are using.)