arrive®
EDGELESS MEDIA

Arrive AirPoint®

Deployment Guide

Arrive AirPoint® Network Deployment Guide

Contents

Doc. Ver.AIDG-802-002

This page left intentionally blank.

COPYRIGHT NOTICE

Disclaimer

THE SPECIFICATIONS, INFORMATION, DESIGNS, STATEMENTS, AND RECOMMENDATIONS (COLLECTIVELY, “INFORMATION”) REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE,AND ALL IMAGES ARE FOR REFERENCE USE ONLY.FINISHED GOODS, PACKAGING,AND PRODUCTS WILL BE PROVIDED WITH USER DESIGNS AND GRAPHIC ELEMENTS INCLUDING PACKAGING DESIGN ELEMENTS THAT MAY VARY FROM THE IMAGES SHOWN IN THIS DOCUMENT.E&OE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS. ARRIVE DISCLAIMS ALL WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE. IN NO EVENT SHALL ARRIVE OR ITS INFORMATION SOURCES AND SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS, LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF ARRIVE OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

ALL TRADEMARKS AND INFORMATION ARE OWNED BY THE RESPECTIVE OWNERS OF THE TRADEMARKS AND INFORMATION, WHETHER ACKNOWLEDGED OR NOT IN THIS DOCUMENT. ARRIVE DOES NOT CLAIM ANY OWNERSHIP OF ANY TRADEMARK OR TRADENAME MENTIONED IN THE INFORMATION EXCEPT FOR THE ARRIVE TRADE NAMES – ARRIVE, ARRIVE FACEPOINT, ARRIVE INFOPOINT, ARRIVE ROOMPOINT, ARRIVE CONTROLPOINT, ARRIVE EYEPOINT, ARRIVE TOUCHPOINT, ARRIVE VIEWPOINT, ARRIVE VOICEPOINT, ARRIVE SOUNDPOINT, ARRIVE ONEPOINT, ARRIVE EDGELESS MEDIA, THE ARRIVE LOGO, ARRIVE MEDIAPOINT, AND ARRIVE AIRPOINT. ITUNES, MAC, AND OS X ARE EITHER TRADEMARKS OR REGISTERED TRADEMARKS OF APPLE, INC. IN THE U.S. AND/OR OTHER COUNTRIES. IOS IS EITHER A TRADEMARK OR REGISTERED TRADEMARK OF CISCO SYSTEMS, INC. IN THE UNITED STATES AND/OR OTHER COUNTRIES. ANDROID AND GOOGLE PLAY ARE EITHER TRADEMARKS OR REGISTERED TRADEMARKS OF GOOGLE, INC. IN THE UNITED STATES AND/OR OTHER COUNTRIES. HDMI IS EITHER A TRADEMARK OR REGISTERED TRADEMARK OF HDMI LICENSING, LLC IN THE UNITED STATES AND/OR OTHER COUNTRIES. EXCEL, MICROSOFT, POWERPOINT, WINDOWS, WINDOWS VISTA,WINDOWS XP, WINDOWS 7, AND WINDOWS 8 ARE EITHER TRADEMARKS OR REGISTERED TRADEMARKS OF MICROSOFT CORPORATION IN THE UNITED STATES AND/OR OTHER COUNTRIES. OTHER TRADEMARKS, REGISTERED TRADEMARKS, AND TRADE NAMES MAY BE USED IN THIS DOCUMENT TO REFER TO EITHER THE ENTITIES CLAIMING THE MARKS AND NAMES OR THEIR PRODUCTS. ARRIVE DISCLAIMS ANY PROPRIETARY INTEREST IN THE MARKS AND NAMES OF OTHERS. ARRIVE IS NOT RESPONSIBLE FOR ERRORS IN TYPOGRAPHY OR PHOTOGRAPHY.

Fictional user of “Visionergy” and/or “Verity” name in examples

Arrive Systems Inc. uses a variety of fictional companies in the documentation and training material for its products. ARRIVE documentation and learning materials often contain fictional scenarios and descriptions of how our products can be deployed and used in these scenarios. Some examples depicted herein such as the corporate name “Visionergy” and/or “Verity”, just like “Contoso” is generally used by Microsoft®. These names are provided for illustration only and are fictitious. No real association or connection is intended or should be inferred. Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

ARRIVE disclaims ownership of the brand or use or association of the name “Visionergy” and/ or “Verity” as a real business or business entity and does not recommend the use of this name by others for a similar purpose of creating examples to avoid confusion. The domain visionergy.com is set to reflect to arrivesys.com.

We reserve the right to introduce changes after the printing of this document. Refer to our website www.arrivesys.com for updated documentation and information.

Document Scope

This document guides the user through the first steps of deploying the Arrive AirPoint®. It provides best practices for implementation including inter-operaion with third-party devices and applications, and other backend infrastructure services required.

Introduction

The wired world that we all know, the one that is connected by miles and miles of cabling, is all changing. The world of WiFi has taken over to spread media sharing love without wires and has proven immensely popular by replacing wired video and audio connections from user devices to connected displays.

In this guide we explain just what Wireless Media Presentation is and why you should be paying attention to it; it does an awful lot today and provides several options for network deployment architecture that you may wish to use in your facilities to enable visual collaboration – anywhere and everywhere.

The Arrive AirPoint™ (AAP) Wireless Media Gateway allows users to present their content via connected projectors and flat panel displays using ad-hoc (peer-to-peer) wireless connections as well as the existing wireless LAN infrastructure without connecting wires or having to download software applications on their personal devices. AAP technology is embedded in several Arrive products which offer standalone or integrated functionality with advanced AV wired switching side by side to Arrive AirPoint wireless media presentation capability.
The Arrive AirPoint is a tiny network video processing device with an in-built wireless access point providing a versatile function with a Universal Wireless Media presentation capability. It supports connections for Apple AirPlay and WiFi Miracast wireless media streaming platforms out-of-the-box with HD video display resolution. This means that compatible Apple, Windows® and Android OS device users can share their on-screen media without having to run any application or attach wires or dongles to their personal devices (no installation or download required).

Arrive AirPoint has been designed with simple set-up and ease of use in mind to provide a true walk-up-and-use experience. The device functions as a receiving end-point much like a wireless printer deployed on a network.
This document provides information on Arrive AirPoint operation, user access, security, and deployment scenarios.

For individual product information, please refer to Quickstart Guides for Arrive devices that have embedded Arrive AirPoint inside.

Arrive offers several options to choose the best way to connect Bring-Your-Own-devices to large display screens in shared work spaces such as huddle rooms, meeting rooms, classrooms and training facilities.

Wouldn’t it be great if you could effortlessly connect your WiFi-enabled devices without messing around with access points and lengthy passphrases? That’s what Arrive’s AirPoint enabled devices promise.

1. Before You Begin

Please refer to separate user guides for AirPoint and MediaPoint hardware devices in terms of hardware installation and connection.

It is also assumed that required hardware set up is complete, and other requirements such as power, network and internet access, as needed, are configured and available.

This AirPoint Network Deployment Guide is applicable for the following Arrive products:

AAP-1011-BYMG

AAP-2011-BYMG

AMP-1041-FTMH

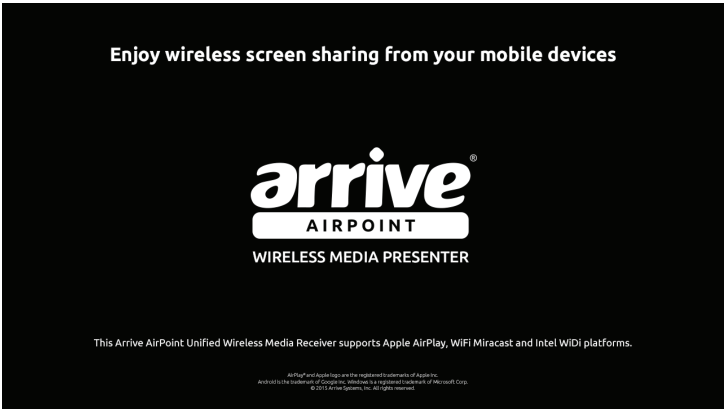
- **AAP-1011-BYMG** AirPoint Media Collaboration Gateway with Wireless BYOD
- **AAP-2011-BYMG** Dual band AirPoint Media Collaboration Gateway with Wireless BYOD
- **AMP-1041-FTMH** Flat-Top MediaPoint Unified Media Collaboration Cable Hub with Wired/Wireless BYOD
- AMP-1041-BYMG MediaPoint Unified Media Collaboration Gateway with Wired/ Wireless BYOD
- AMP-1041-BYMH Tilt-Top MediaPoint Unified Media Collaboration Cable Hub with Wired/Wireless BYOD

Review the products' specification sheets (download at http://www.arrivesys.com), installation guides, and user guides (download from the Arrive Partner Portal) for more information.

2. User Experience

On-Screen Display

Arrive AirPoint uses an on-screen display to convey the basic connection instructions for wireless access to the device. The splash screen is standardized and appears as a default tutorial. It provides the hostname, IP address, and SSID login code for the specific Arrive AirPoint device.

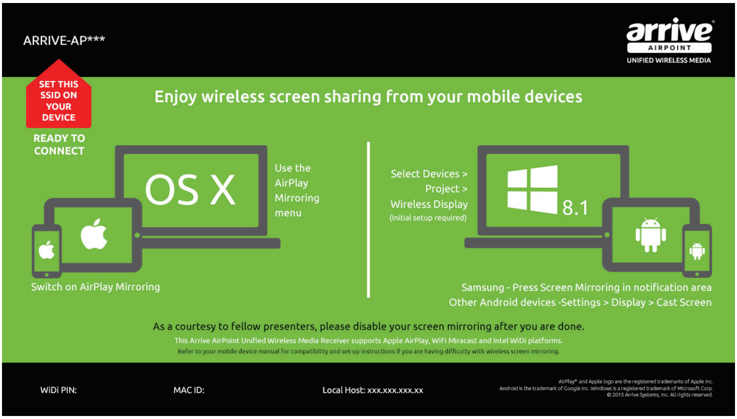

Enjoy wireless screen sharing from your mobile devices

This Arrive AirPoint Unified Wireless Media Receiver supports Apple AirPlay, WiFi Miracast and Intel WiDi platforms.

AirPlay® and Apple logo are the registered trademarks of Apple Inc.
Android is the trademark of Google Inc. Windows is a registered trademark of Microsoft Corp.
© 2015 Arrive Systems, Inc. All rights reserved.

Figure 1: Boot-up screen

The boot-up screen transitions to the ready-to-connect user tutorial screen which, by default uses the Peer-toPeer mode, signifying that the device is ready to receive wireless communications.


ARRIVE-AP***

Enjoy wireless screen sharing from your mobile devices

Use the AirPlay Mirroring menu

Switch on AirPlay Mirroring

Select Devices > Project > Wireless Display
(Initial setup required)

Samsung - Press Screen Mirroring in notification area
Other Android devices -Settings > Display > Cast Screen

As a courtesy to fellow presenters, please disable your screen mirroring after you are done.
This Arrive AirPoint Unified Wireless Media Receiver supports Apple AirPlay, WiFi Miracast and Intel WiDi platforms.
Refer to your mobile device manual for compatibility and set-up instructions if you are having difficulty with wireless screen mirroring.

WiDi PIN:

MAC ID:

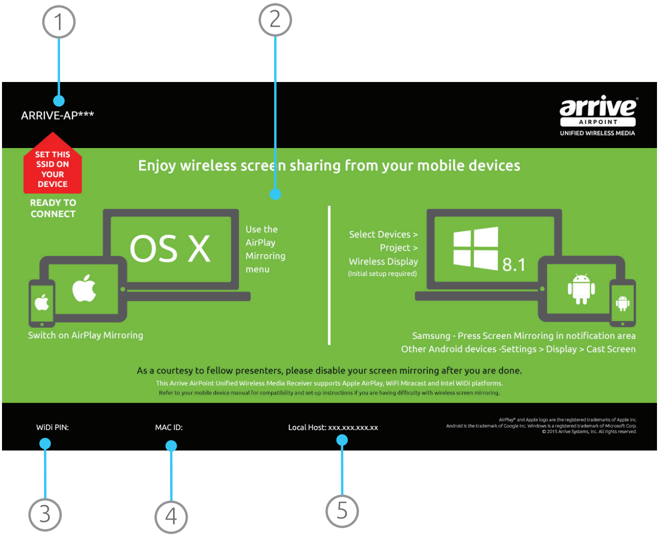
Local Host: xxx.xxx.xxx.xx

AirPlay® and Apple logo are the registered trademarks of Apple Inc.
Android is the trademark of Google Inc. Windows is a registered trademark of Microsoft Corp.
© 2015 Arrive Systems, Inc. All rights reserved.

Figure 2: User tutorial screen

Figures 3 and 4 discusses the various parts of the user tutorial screen :

3. Peer-to-Peer mode:


1
2
3
4
5
ARRIVE-AP***
arrive AIRPOINT
UNIFIED WIRELESS MEDIA
SET THIS SSID ON YOUR DEVICE
READY TO CONNECT
OS X
Use the AirPlay Mirroring menu
Switch on AirPlay Mirroring
Select Devices > Project > Wireless Display
(Initial setup required)
8.1
WiDi PIN:
MAC ID:
Local Host: xxx.xxx.xxx.xx

Enjoy wireless screen sharing from your mobile devices

Samsung - Press Screen Mirroring in notification area

Other Android devices -Settings > Display > Cast Screen

As a courtesy to fellow presenters, please disable your screen mirroring after you are done.

This Arrive AirPoint Unified Wireless Media Receiver supports Apple AirPlay, WiFi Miracast and Intel WiDi platforms.

Refer to your mobile device manual for compatibility and set-up instructions if you are having difficulty with wireless screen mirroring.

AirPlay® and Apple logo are the registered trademarks of Apple Inc.
Android is the trademark of Google Inc. Windows is a registered trademark of Microsoft Corp.
© 2015 Arrive Systems, Inc. All rights reserved.

Figure 3: Peer-to-Peer mode tutorial screen

Review Figure 3 with the definitions below:

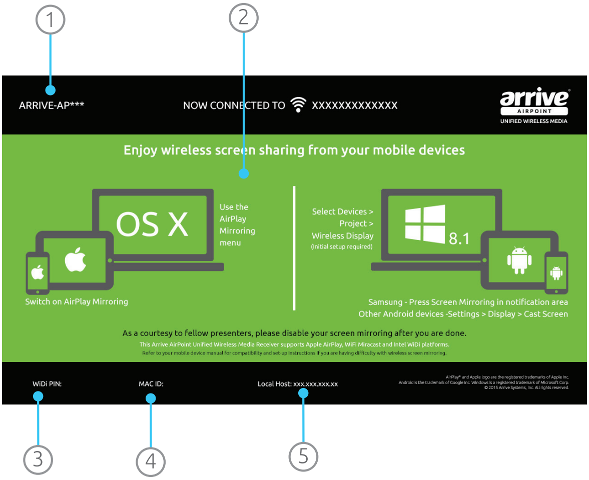
1. Enable wireless settings on your device and select this SSID. This SSID is not constant, and will change from time-to-time.
2. This graphics provides a quick summary of how to connect various devices to Arrive AirPoint.
3. Enter the PIN number here if you are connecting via Intel WIDI.
4. This is just for information and not required by users.
5. The Arrive AirPoint runs an internal webserver. This is the IP address of that webserver. Should be used only by the System Administrator to setup the Arrive AirPoint.

Note: PLEASE REMEMBER THAT YOU NEED TO DISCONNECT YOUR BYOD MEDIA FROM THE SCREEN TO ALLOW OTHERS TO CONNECT.

SSID login code:

Each device has a unique SSID code. This unique SSID login code is provided to ensure users connect to the display screen they wish to display their media on. It also provides the ability for two or more of the Arrive AirPoint devices to be available in the same space. The user needs to connect to the specific SSID before the attached display will accept the wireless media display.

4. WiFi-connected mode:



ARRIVE-AP***

NOW CONNECTED TO XXXXXXXXXXXX

UNIFIED WIRELESS MEDIA

Enjoy wireless screen sharing from your mobile devices

Use the AirPlay Mirroring menu

Switch on AirPlay Mirroring

Select Devices > Project > Wireless Display (Initial setup required)

Samsung - Press Screen Mirroring in notification area
Other Android devices -Settings > Display > Cast Screen

As a courtesy to fellow presenters, please disable your screen mirroring after you are done.
This Arrive AirPoint Unified Wireless Media Receiver supports Apple AirPlay, WiFi Miracast and Intel WiDi platforms.
Refer to your mobile device manual for compatibility and set-up instructions if you are having difficulty with wireless screen mirroring.

WiDi PIN:

MAC ID:

Local Host: xxx.xxx.xxx.xx

AirPlay® and Apple logo are the registered trademarks of Apple Inc.
Android is the trademark of Google Inc. Windows is a registered trademark of Microsoft Corp.
© 2015 Arrive Systems, Inc. All rights reserved.

Figure 4: WiFi connected mode tutorial screen

Review Figure 4 with the definitions below:

1. Enable wireless settings on your device and select this SSID. This SSID is not constant, and will change from time-to-time.
2. This graphics provides a quick summary of how to connect various devices to Arrive AirPoint.
3. Enter the PIN number here if you are connecting via Intel WIDI.
4. This is just for information and not required by users.
5. The Arrive AirPoint runs an internal webserver. This is the IP address of that webserver. Should be used only by the System Administrator to setup the Arrive AirPoint. When connected to the WiFI network, the webserver IP address will change from the default address.

Note: AS WITH THE CASE OF PEER-TO-PEER MODE, REMEMBER THAT YOU NEED TO DISCONNECT YOUR BYOD MEDIA FROM THE SCREEN TO ALLOW OTHERS TO CONNECT IN THE WIFI-CONNECTED MODE.

WiFi SSID and Unique ID login code

In WiFi Connected mode, the words " Now connected to ________", appear signifying that the Arrive AirPoint device is connected to the WiFi network. In this mode the AirPoint device's own SSID is invisible and the Arrive AP**** ID serves as a ID for the user to select for connection using Apple AirPlay or WiFi Miracast. This unique ID login code is provided to ensure users connect to the display screen they wish to display their media on. It also provides the ability for two or more of the Arrive AirPoint devices to be available in the same space. The user needs to ensure that they are connected to the same WiFi LAN infrastructure as the Arrive AirPoint device and then select the unique device ID before the attached display will accept the wireless media display.

4.1 Arrive AirPoint Deployment within Enterprise and Campus WiFi infrastructure

Enterprise Deployment Options for User Network Access

In secured enterprise and campus networks there will generally be a requirement to provide two types of users access to the Arrive AirPoint embedded devices for allowing wireless media presentation to be made in meeting rooms, huddle rooms, classrooms and other shared workspace facilities.

1. Authorized Users with access to the enterprise or campus LAN.
2. Guest users who do not have access to the enterprise or campus LAN.

Guests may want to present to enterprise and campus authorized network users. Keeping the guest networks and corporate networks separate while allowing the users to share a display presents a challenge in the world of wireless BYOD when the wireless network is part of the secured infrastructure.

As a standards based WiFi network device, Arrive AirPoint solves this problem by using standard networking practices. There are three suggested methods:

1. Virtual AP - Ad-hoc Network based Method (AirPoint acts as a standalone WiFi access point)
2. WiFi Connected - VLAN based Method (AirPoint joins your enterprise WiFi network as a client)
3. Physical Air Wall Method (two AirPoint devices join your enterprise WiFi network as separate clients one for secure access users and the other for guest users)

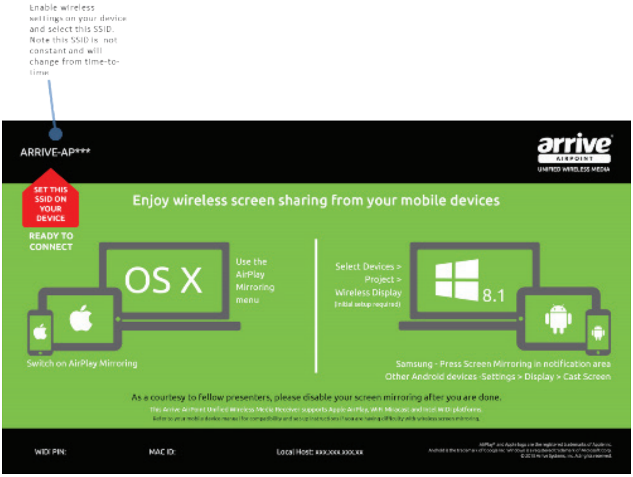
4.2 Virtual AP - Ad-Hoc Peer-to-Peer WiFi based connection Method

A wireless ad-hoc Peer-to-Peer (P2P) WiFi connection to Arrive AirPoint devices, is a standalone one way device-bound wireless network connection.

In this mode the Arrive AirPoint device acts as a media receiver allowing only single incoming connections. Multiple connections are not possible. The network is ad hoc because it does not rely on a pre-existing infrastructure, such as routers in wired networks or access points in managed (infrastructure) wireless networks. Instead, each device provides the ability for a one-way receiving only network connection to be made with connected mobile and user wireless devices such as smart phones, tablets and laptops equipped with a compatible

802.11 WiFi capability.

This method presents the highest level of security and treats both Authorized Users and Guest Users the same.



Enable wireless settings on your device and select this SSID. Note this SSID is not constant and will change from time-to-time

ARRIVE-AP***

SET THIS SSID ON YOUR DEVICE

READY TO CONNECT

Enjoy wireless screen sharing from your mobile devices

Use the AirPlay Mirroring menu

Switch on AirPlay Mirroring

Select Devices > Project > Wireless Display (initial setup required)

Samsung - Press Screen Mirroring in notification area
Other Android devices -Settings > Display > Cast Screen

As a courtesy to fellow presenters, please disable your screen mirroring after you are done.

This Arrive AirPoint Unified Wireless Media Receiver supports Apple AirPlay, WiFi Miracast and Intel WiDi platforms.
Refer to your mobile device manual for compatibility and setup instructions if you are having difficulty with wireless screen mirroring.

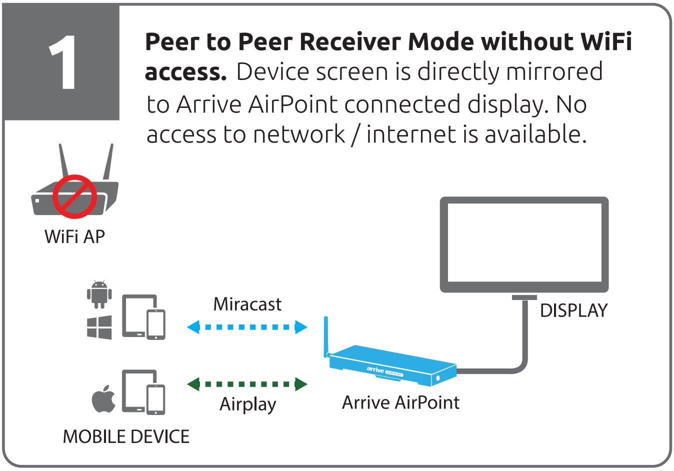
WIDI PIN:

MAC ID:

Local Host: xxx.xxx.xxx.xx

Figure 5: Finding the SSID

Peer-to-Peer Receiver Mode without WiFi access

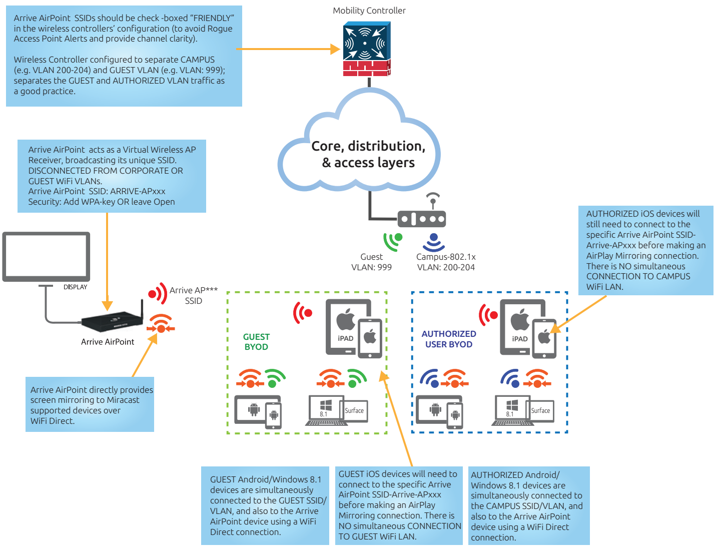


1

Peer to Peer Receiver Mode without WiFi access. Device screen is directly mirrored to Arrive AirPoint connected display. No access to network / internet is available.

Figure 6: Peer-to-Peer Receiver mode without WiFi access topology

AD-HOC WiFi MODE: Arrive AirPoint devices are disconnected from the WiFi LAN. Each AirPoint device broadcasts its own SSID independent of the WiFi LAN network.



Arrive AirPoint SSIDs should be check -boxed "FRIENDLY" in the wireless controllers' configuration (to avoid Rogue Access Point Alerts and provide channel clarity).

Wireless Controller configured to separate CAMPUS (e.g. VLAN 200-204) and GUEST VLAN (e.g. VLAN: 999); separates the GUEST and AUTHORIZED VLAN traffic as a good practice.

Arrive AirPoint acts as a Virtual Wireless AP Receiver, broadcasting its unique SSID. DISCONNECTED FROM CORPORATE OR GUEST WiFi VLANs.
Arrive AirPoint SSID: ARRIVE-APxxx
Security: Add WPA-key OR leave Open

Arrive AirPoint directly provides screen mirroring to Miracast supported devices over WiFi Direct.

AUTHORIZED iOS devices will still need to connect to the specific Arrive AirPoint SSID-Arrive-APxxx before making an AirPlay Mirroring connection. There is NO simultaneous CONNECTION TO CAMPUS WiFi LAN.

GUEST Android/Windows 8.1 devices are simultaneously connected to the GUEST SSID/VLAN, and also to the Arrive AirPoint device using a WiFi Direct connection.

GUEST iOS devices will need to connect to the specific Arrive AirPoint SSID-Arrive-APxxx before making an AirPlay Mirroring connection. There is NO simultaneous CONNECTION TO GUEST WiFi LAN.

AUTHORIZED Android/Windows 8.1 devices are simultaneously connected to the CAMPUS SSID/VLAN, and also to the Arrive AirPoint device using a WiFi Direct connection.

Figure 7: AirPoInt as virtual wireless AP receiver

In Figures 8-7, it shows that:

1. The Arrive AirPoint device has no network or internet connection of its own.
2. Arrive AirPoint acts as a native receiver for both Apple AirPlay and WiFi Miracast capable user devices. Please read detailed information on Apple AirPlay and WiFi Miracast technologies later in this guide to better understand how these technologies work and their individual capabilities.
3. The visual experience for the users depends upon the type of user device they are connecting to the Arrive AirPoint appliance.
   - In this mode connected Apple Airplay devices have the limitation of having no access to the internet over the dedicated WiFi connection and therefore only media residing on the user device such as presentations, photos and videos and local applications can be shared over the Arrive AirPoint. Apple devices can retain the internet connection via their individual data plans from the mobile service provider over 4G LTE or 3G networks and this will allow for both Internet and the WiFi AirPlay Screen mirroring to function together.
   - On the other hand all WiFi Miracast compatible devices will be able to use WiFi direct to enable multi-connect capability. So these devices will have both the WiFi network connection as well as the Peer-to-Peer wireless media connection as the

same time.

4. The connection is One-on-One – One device to one Arrive AirPoint Receiver at one time. The connected device has to disconnect before another device can connect.
5. While a connection is “live” the Arrive AirPoint Receiver unique SSID becomes invisible from other devices and also does not allow access to its settings (the IP address is invisible) – in other words it becomes a dedicated receiver for the connected device for the duration of the live connection.
6. As soon as the live connection is disconnected, the AirPoint SSID and IP address become visible indicating that the device is ready to connect.

In summary :

1. The device in P2P mode acts as a wireless media receiver for AirPlay and Miracast connections. This is a one way connection.
2. This is the simplest plug-and-play out of the box capability without requiring any configuration or setup.
3. The device is completely secured as it does not have any access to outside networks and also not connected to the internet.
4. The device SSID is broadcasted and visible to BYOD devices for connection.
5. Since the device is not part of the WiFi network it does not need to abide by firewall or other group policies.
6. This mode has no dependence on the WiFi LAN network performance and therefore exhibits low latency.
7. Only in the case of Apple AirPlay connections are users inconvenienced with no internet access via WiFi. Other users who BYOD Miracast capable devices (Windows 8.1 and Android) do not have this inconvenience as their devices have the ability to have a dual connection using WiFi Direct to the Arrive AirPoint.

Note: ARRIVE AIRPOINT IN P2P MODE IS A MEDIA RECEIVING DEVICE ADVERTISING AN SSID FOR WIRELESS PRESENTATION, WITHOUT A CONNECTION TO ANY OTHER NETWORK.

WHEN USED IN THIS MODE THE AIRPOINT IS NOT A HONEYPOT.

For IT Network Managers:

The Arrive AirPoint devices in peer-to-peer mode will appear as independent Virtual 2.4 Ghz* WiFi Access Points. It does not have any other connection to enterprise network. IT network and security specialists should know more before mass deployment decisions are made. The discussion given below is meant to shed some light on the P2P device mode connection.

1. Security Risk Assessment: Arrive AirPoint wireless in P2P mode operates as a tiny access point advertising its unique SSID. This SSID is visible in the room where the AirPoint is installed and with a radius of 10 to 15 feet from the device.

   Generally, IT security policies would not allow an unmanaged AP which can be misused to connect to corporate LAN/WAN or internet. With the Arrive AirPoint devices in P2P mode its impossible to establish a connection to your enterprise wireless network. It also does not have any other connection leg to any other network. Any user connecting to Arrive AirPoint SSID will not be able to receive any service other than AirPoint wireless presentation sharing capability which only connects with AirPlay or Miracast capable devices and only one at a time. Multiple connections are not possible and the mode is receiver mode. So even if user devices can connect to the Arrive AirPoint, they cannot do anything with this connection other than screen mirroring.

2. Wireless RF Concerns: Rogue access points are generally identified as a wireless SSID which doesn't belong to an enterprise network. You may see rogue access point in an enterprise, from people using a personal device on a data plan to tether from their phablets.

Your WiFi security team will have full visibility of Arrive AirPoint devices on the wireless controller and these may be identified as "rogue".

Advice: Arrive AirPoint in P2P mode broadcasts its SSID and operates on specific 2.4 GHz channel* The radio managment module of your wireless controller tunes your WiFi to avoid interference with AirPoint.

WHEN USED IN THIS MODE WIFI USERS WILL SEE THE AIRPOINT SSID ON THEIR DEVICES.

It will be prudent to inform users about the function of Arrive AirPoint SSID and its function as a standalone wireless presentation device and that it does not provide internet access to Apple iOS Airplay devices in this mode.

The AirPoint device, unlike a personal tethered device cannot cause RF harm to your network as it only operates on a single specific 2.4Ghz* channel and doesn't change its frequency. The radio management system of your wireless controller (such as Cisco CleanAir, Aruba ARM , HP RRM) will tune your enterprise wireless RF network to avoid interference with Arrive AirPoint installed in the rooms. If this is an acceptable outcome of the deployment use case for several Arrive AirPoint devices in Peer-to-Peer Ad-hoc mode, it would be prudent to define the AirPoint SSIDs detected in the wireless controller as a Safe/ Friendly AP so the controller doesn't keep alarming you.

* For AAP-1011-BYMG and AMP-1041-FTMH models only. AAP-2011-BYMG operates on both 2.4 and 5GHz channels.

WiFi Connected Mode

2

Peer to Peer Receiver with WiFi access only by Arrive AirPoint. Device screen is directly mirrored to Arrive AirPoint connected display. Device has network / internet access via Arrive AirPoint.

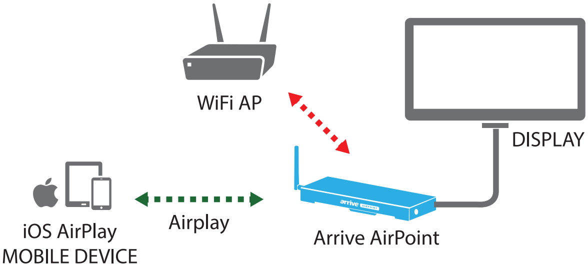


Figure 8: WiFi connected mode topology

The WiFi mode allows the device to become part of the WiFi local area network infrastructure and act as a virtual wireless access point. Similar to user devices that need to connect to the secured WiFi network, the Arrive AirPoint needs the existence of a WiFi LAN network SSID and WPA security key to be configured on each device - one-time. It always connects to this SSID.

a. In the WiFi-C mode, the device does not broadcast its own SSID, instead it uses the connected WiFi LAN SSID.

b. BYOD devices connect to the WiFi LAN and are able to discover the device as an AirPlay or Miracast media receiver. By selecting the specific device ID, the user is able to select the screen to which they wish to mirror their BYOD devices.

c. All policies, encryptions, and other security measures implemented carry over to Arrive AirPoint because it creates standard Ethernet traffic. Once on the enterprise or campus network, the traffic generated by Arrive AirPoint is treated like any other network traffic. All existing policies that apply to physical network devices (switches, routers, etc.) also apply to Arrive AirPoint. Arrive AirPoint can be treated as a standard network appliance (like a printer) and is as secure as the supporting network.

d. This type of connection induces latency on the connection based on the WiFi performance.

5. VLAN Based Secure Provisioning

In this method, Arrive AirPoint devices join the enterprise wireless network, within a contained SSID and VLAN. Arrive AirPoint supports WPA/WPA2-PSK (pre-shared key).

A specific SSID and VLAN is created on your wireless controller with WPA2 PSK security configuration. Additionally one may consider adding MAC address based authentication to ensure only the Arrive AirPoint devices are connected to this SSID. (Arrive AirPoint MAC Addresses are available from the On Screen Display).

The Wireless controller and firewall needs to get configured in a way to block the traffic from this VLAN (subnet) towards your corporate/campus network and optionally to internet . Arrive AirPoint has a AirPlay receiver which uses Bonjour protocol to advertise its capabilities. The Bonjour protocol is a non-routable protocol. Arrive AirPoint device is configured to connect to the enterprise WiFi LAN using a SSID/VLAN and Secure WPA/WPA2 key (one time configuration required).

Wireless controller mDNS listener for this VLAN must be enabled, and VLAN is configured to only allow incoming connections (based on your wireless controller configurations). Outbound traffic is not allowed.

To segregate users it will be important for you to ensure that the guest and corporate networks exist in separate SSID/VLANs.

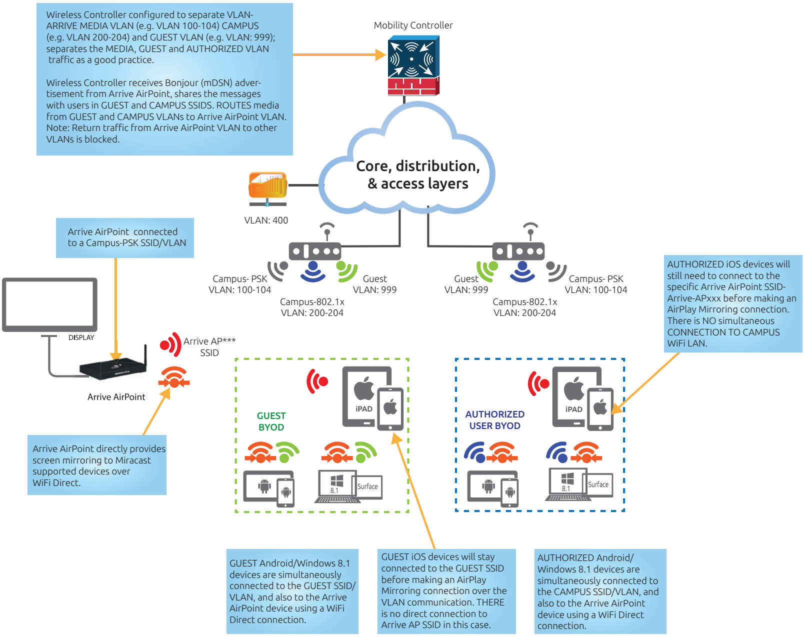
Your wireless controller listens for Bonjour mDNS advertisements from AirPoints installed in different rooms. The Wireless controller caches the information (List of AirPoints , IP addresses and MAC addresses).

[1] Arrive AirPoint requires to connect to internet for OTA (Over The Air software update). Blocking the internet access will stop the AirPoint from receiving the new firmware and patches.

The Apple BYOD devices in GUEST or the Corporate SSID send request for list of available services. Wireless controller sends the list of Arrive AirPoints to the user devices which are located in GUEST or Corporate wireless SSID/ VLAN.

Once the Apple iPhone/iPAD receives the list of devices from controller, it shows as the list of available Mirroring displays.

WiFi VLAN CONNECTED: Arrive AirPoint device is connected to the WiFi network using a separate VLAN



Wireless Controller configured to separate VLAN- ARRIVE MEDIA VLAN (e.g. VLAN 100-104) CAMPUS (e.g. VLAN 200-204) and GUEST VLAN (e.g. VLAN: 999); separates the MEDIA, GUEST and AUTHORIZED VLAN traffic as a good practice.

Wireless Controller receives Bonjour (mDSN) advertisement from Arrive AirPoint, shares the messages with users in GUEST and CAMPUS SSIDS. ROUTES media from GUEST and CAMPUS VLANs to Arrive AirPoint VLAN. Note: Return traffic from Arrive AirPoint VLAN to other VLANs is blocked.

Arrive AirPoint connected to a Campus-PSK SSID/VLAN

AUTHORIZED iOS devices will still need to connect to the specific Arrive AirPoint SSID- Arrive-APxxx before making an AirPlay Mirroring connection. There is NO simultaneous CONNECTION TO CAMPUS WiFi LAN.

Arrive AirPoint directly provides screen mirroring to Miracast supported devices over WiFi Direct.

GUEST Android/Windows 8.1 devices are simultaneously connected to the GUEST SSID/ VLAN, and also to the Arrive AirPoint device using a WiFi Direct connection.

GUEST iOS devices will stay connected to the GUEST SSID before making an AirPlay Mirroring connection over the VLAN communication. THERE is no direct connection to Arrive AP SSID in this case.

AUTHORIZED Android/ Windows 8.1 devices are simultaneously connected to the CAMPUS SSID/VLAN, and also to the Arrive AirPoint device using a WiFi Direct connection.

Figure 9: Configuring a wireless controller

Note: For more detailed information about configuring your wireless controller please refer to your vendor web site.

5.1 Aruba ClearPass :

Aruba has created enhanced AirGroup features within Aruba ClearPass which allows the administrator to restrict the Arrive AirPoint advertisement per room / floor. When users will open a AirPlay connection from their connected iOS device, they will see only the AirPoint devices in the room / floor as configured without cluttering the entire list of Arrive AirPoints connected to the network.

For more details refer to AirGroup Configuration at:

Aruba AirGroup configuration: http://bit.ly/1aNcQL5

5.2 Cisco Bonjour Gateway:

Bonjour is Apple’s service discovery protocol which locates devices such as printers, other computers, and the services that those devices offer on a local network using multicast Domain Name System (mDNS) service records.

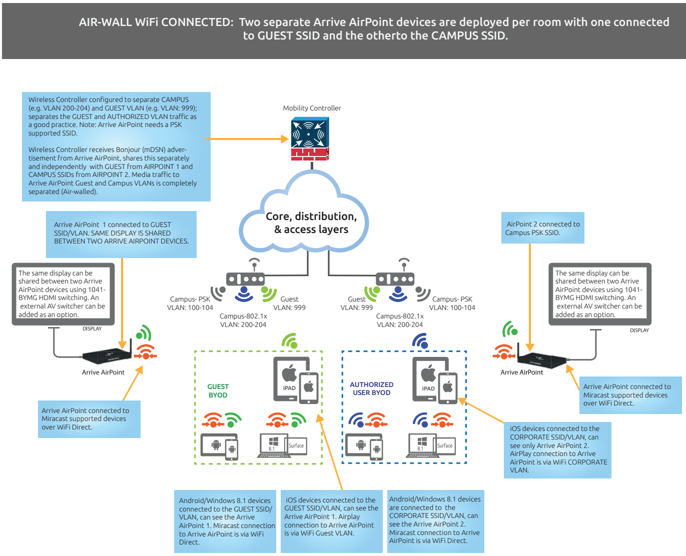
The Cisco Wireless LAN Controller acts as a Bonjour Gateway. The WLC listens for Bonjour services and by caching those Bonjour advertisements (AirPlay, AirPrint etc.) from the source/ host e.g. AppleTV, responds back to Bonjour clients when a request for service is initiated.

Cisco Bonjour gateway information: http://bit.ly/1P9Go5g

6. Physical Air Wall Method

The concept of an “air wall (also called air-gap)” in computing refers to the idea of isolating a computer installation to make it extraordinarily secure--so much so that it could almost be considered a closed system. In this method, the corporate and guest networks are separated by a physical air wall/gap.

To make it convenient without having to add several interfaces, two Arrive AirPoint embedded devices are used: one for corporate users and one for guest users. Switching presentations is done in the HDMI domain by using 1 x Arrive AMP-1041-BYMG or BYMH wired and wireless media hub and a second AAP-1011-BYMG as the guest wireless gateway (this eliminates using an external HDMI switcher). While extremely secure, this approach requires more hardware between the two devices and their respective HDMI outputs (IR, Button Panel and RS-232 control available).


AIR-WALL WiFi CONNECTED: Two separate Arrive AirPoint devices are deployed per room with one connected to GUEST SSID and the otherto the CAMPUS SSID.

Wireless Controller configured to separate CAMPUS (e.g. VLAN 200-204) and GUEST VLAN (e.g. VLAN: 999); separates the GUEST and AUTHORIZED VLAN traffic as a good practice. Note: Arrive AirPoint needs a PSK supported SSID.

Wireless Controller receives Bonjour (mDSN) advertisement from Arrive AirPoint, shares this separately and independently with GUEST from AIRPOINT 1 and CAMPUS SSIDs from AIRPOINT 2. Media traffic to Arrive AirPoint Guest and Campus VLANs is completely separated (Air-walled).

Arrive AirPoint 1 connected to GUEST SSID/VLAN. SAME DISPLAY IS SHARED BETWEEN TWO ARRIVE AIRPOINT DEVICES.

The same display can be shared between two Arrive AirPoint devices using 1041-BYMG HDMI switching. An external AV switcher can be added as an option.

Arrive AirPoint connected to Miracast supported devices over WiFi Direct.

AirPoint 2 connected to Campus PSK SSID.

The same display can be shared between two Arrive AirPoint devices using 1041-BYMG HDMI switching. An external AV switcher can be added as an option.

Arrive AirPoint connected to Miracast supported devices over WiFi Direct.

iOS devices connected to the CORPORATE SSID/VLAN, can see only Arrive AirPoint 2. AirPlay connection to Arrive AirPoint is via WiFi CORPORATE VLAN.

Android/Windows 8.1 devices connected to the GUEST SSID/ VLAN, can see the Arrive AirPoint 1. Miracast connection to Arrive AirPoint is via WiFi Direct.

iOS devices connected to the GUEST SSID/VLAN, can see the Arrive AirPoint 1. Airplay connection to Arrive AirPoint is via WiFi Guest VLAN.

Android/Windows 8.1 devices are connected to the CORPORATE SSID/VLAN, can see the Arrive AirPoint 2. Miracast connection to Arrive AirPoint is via WiFi Direct.

Figure 10: Physical Air-Wall method

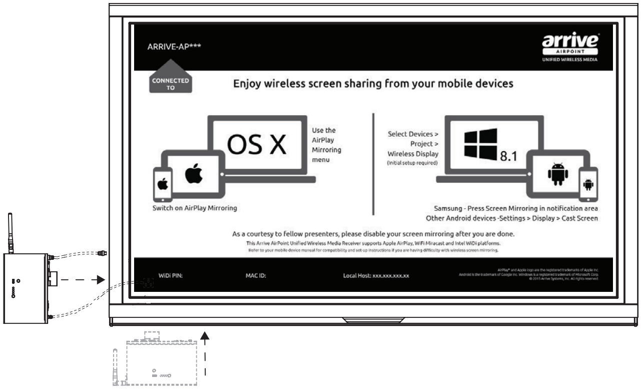
7. Captive Internet Portals

In WiFi connected mode the Arrive AirPoint does not provide access to captive internet portals. Providing internet or network access in WiFi enterprise or campus LAN's will require a WPA /WPA2 security key to be available for configuring on the Arrive AirPoint device. If your infrastructure supports and mandates captive internet portals, you will need to discuss and set-up a bypass policy for Arrive AirPoint devices to access the internet. One of the ways to achieve a bypass of a captive portal would be to exempt the MAC address of network attached Arrive AirPoint clients.

8. Mounting Tips for Arrive Wireless Media Gateways and Hubs

8.1 Device Placement

Where you should place your Arrive AirPoint and Arrive MediaPoint wireless BYOD supported devices depends primarily on the location of where connected users will be most likely to be situated. Other considerations that will affect the location are nearness to power and also the distance from the HDMI capable display that you will connect the device to, as the length of the HDMI cable affects the quality of visual experience. Depending on these locations and dependencies, you should find the position best suited for locating the Arrive device based on the model that you have purchased.



Enjoy wireless screen sharing from your mobile devices

Use the AirPlay Mirroring menu

Switch on AirPlay Mirroring

Select Devices > Project > Wireless Display (Initial setup required)

Samsung - Press Screen Mirroring in notification area
Other Android devices -Settings > Display > Cast Screen

As a courtesy to fellow presenters, please disable your screen mirroring after you are done.

This Arrive AirPoint Unified Wireless Media Receiver supports Apple AirPlay, WiFi Miracast and Intel WiDi platforms.

Refer to your mobile device manual for compatibility and set-up instructions if you are having difficulty with wireless screen mirroring.

AirPlay® and Apple logo are the registered trademarks of Apple Inc.
Android is the trademark of Google Inc. Windows is a registered trademark of Microsoft Corp.
© 2015 Arrive Systems, Inc. All rights reserved.

Figure 11: Wall-mounting for AAP-1011-BYMG

It is recommended that the AirPoint devices be installed on a location where the reset button can be easily reached. Models come with a wall-mounting bracket for easy installation, and the antenna can be adjusted as required.

In general the Arrive MediaPoint hubs are meant to be furniture mounted on podiums and table-tops, therefore the natural location of these models are a given. The AirPoint and

MediaPoint gateway devices are meant to be wall mounted and the best locations will be generally user accessible locations below or beside the displays to allow for a manual wireless reset to take place.

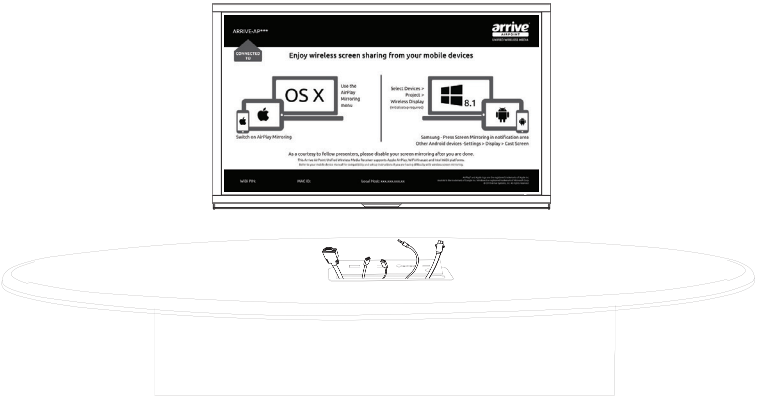

ARRIVE-AP***
arrive
AIRPOINT
UNIFIED WIRELESS MEDIA
CONNECTED TO
Enjoy wireless screen sharing from your mobile devices
OS X
Use the AirPlay Mirroring menu
Switch on AirPlay Mirroring
Select Devices > Project > Wireless Display
(initial setup required)
8.1
Samsung - Press Screen Mirroring in notification area
Other Android devices -Settings > Display > Cast Screen
As a courtesy to fellow presenters, please disable your screen mirroring after you are done.
This Arrive AirPoint Unified Wireless Media Receiver supports Apple AirPlay, WiFi Miracast and Intel WiDi platforms.
WiDi PIN:
MAC ID:
Local Host: xxx.xxx.xxx.xx

Figure 12: MediaPoint hub installed on a table

8.2 Areas to Avoid

For Wireless Gateway Devices :

When placing your gateway device, avoid positioning at a height lower than large furniture pieces, cabinets or other items that may surround the installation area. Generally speaking, the higher the elevation of the device, the better the signal it transmits.

Consequently, placing the device near the ceiling helps reduce interference and usually provides the best signal. Avoid areas where signals from the devices may bounce off mirrors, windows or stainless steel surfaces and those where the WiFi signal may degrade due to thick walls made of brick, concrete or plaster.

The recommended user device distance from the ceiling or wall mounted gateway devices is between 8 ft. to 15 ft. from the device, however, this may vary based on the obstruction and several other considerations of where you have mounted the device. If users face signal management issues based on distance, please always recommend users to get as close to the device location as possible.

8.3 For Furniture Mounted MediaPoint Hub Devices :

Since these devices are meant to be mounted on furniture you cannot avoid positioning these devices at a height lower than large furniture pieces, cabinets or other items that may surround the installation area. MediaPoint hub devices will therefore have a severely restricted range and users are generally required to be sitting or standing near the devices to be able to get the best streaming transmission experience. The recommended distance is between 4 ft. to 12 ft. from the hub, however, this may vary based on the obstruction under the table or furniture where you have mounted the device. In general, we recommend that the under table area is as unobstructed as possible to allow for the wireless device to function properly. In severely affected locations, you have no choice but to find an alternate location before installation is made. Unfortunately, we do not have a scientific method of providing a calculation since the variables are too many. As a best practice a pre-install test is recommended to be conducted before final installation is made by placing and powering the device under the furniture and testing the area of operation and then deciding if this is suitable or not for the venue size and location where users are most likely to be situated.

To provide some performance optimization, Arrive offers two types of antennas with its AMP-1041-BYMH and AMP-1041-FTMH device platforms. The devices are shipped with a 3db and 5db antenna and based on the installation considerations required, the installer can test the WiFi performance and augment the range in severely affected installations by using the higher strength 5db antenna. Arrive generally recommends the use of the 3db antenna.

8.4 Aiming the Antenna

You should aim it in the direction of the area where you use most of your WiFi devices if possible. If you install the gateway devices in the center of the room it may be best in terms of signal, however, the HDMI distance and location of power would then determine the practical location of the device that just the center of the venue. Pointing the antenna straight up in the case of wall mount, L-shaped pointing down in the case of ceiling installs or out in the unobstructed direction for the media hubs below the furniture, may provide the best overall signal. In many cases, you may find it works best to aim the antenna towards your primary WiFi usage area or straight out in a centralized location..

8.5 Other Tips

Other things you can do to improve wireless performance are to ensure that you avoid placing the device near other electrical devices that may cause interference with the WiFi signal. Electric fans, items with motors, microwave, fluorescent lighting and wireless phones are all common causes of WiFi signal interference. Some of these are avoidable and consideration should be made while deciding the location of the wireless gateway or hub device to avoid these as far as possible.

WiFi Connection

- Check for wireless network interferences. It's likely that your wireless controller can show you how crowded your location is. Try to change the channel of the connection.
- Make sure to use the fast 802.11n mode (not b/g) set to 2.4 Ghz.
- Try to ensure that the WiFi access point and Arrive AirPoint device are near (position them as close as possible)
- Turn off bluetooth on your BYOD while presenting (just to make sure that there aren't any interferences)

9. About Apple AirPlay

AirPlay is often compared to DLNA, which is an open system where users can stream music, photos and movies (not games) between devices. DLNA is incorporated into for example TVs, Blu-ray players, tablets, smart phones and more. But AirPlay bears little resemblance to DLNA. It is fundamentally different and only a very small portion of the AirPlay system is similar. The rest is quite unique and not available from any other manufacturer today and you need to understand that AirPlay is just not the same as DLNA.

In order to understand the AirPlay system it is necessary to divide it into two components:

1. AirPlay
2. AirPlay Mirroring

For our documentation purposes we are focusing specifically on AirPlay Mirroring which is the capability that is integrated in Arrive AirPoint systems.

AirPlay Mirroring

AirPlay Mirroring enables users of certain AirPlay-compatible devices to display whatever is on their device's screen on AirPlay-compatible Arrive AirPoint Receivers. This allows users to show presentations, website, video, or other content on their device's screen on a big screen display that the Arrive AirPoint device is attached to. This is achieved via WiFi. Apple Devices that support Airplay Mirroring are:

- from iPhone 4s and later models
- from iPad 2 and later models

A supported Mac

AirPlay Mirroring in OS X takes advantage of the hardware capabilities of recent Macs to deliver high frame rates while maintaining optimal system performance. The following Mac models support AirPlay Mirroring when using OS X Mountain Lion or later:

- iMac (from Mid 2011 or later)
- Mac mini (from Mid 2011 or later)
- MacBook Air (from Mid 2011 or later)
- MacBook Pro (from Early 2011 or later)
- Mac Pro (from Late 2013 or later)

How AirPlay mirroring works

Figure 13: Apple AirPlay mirroring with Arrive MediaPoint

AirPlay and AirPlay Mirroring are two separate elements of Apple's streaming system.

AirPlay Mirroring is different than AirPlay in a number of areas. AirPlay Mirroring establishes a video stream based on the H.246 video format that is continuously being streamed to the Arrive AirPoint device box (and sent to the TV screen). This H.246 stream is created inside the graphic card at the same time as the video stream for the actual iOS screen is created, and that is why AirPlay Mirroring only works on newer Apple devices. What is important to understand is that this approach enables the video stream to be streamed directly to the Arrive AirPoint device with minimal delay. When connected to a WiFi network, the Apple device also gets Internet access while streaming the media, however, the performance is limited by the capability of the WiFi infrastructure. Again, the faster the WiFi network, the better, as WiFi reliability is actually the real bottleneck here. Unlike Miracast, Apple AirPlay does not support WiFi Direct, the reliance on the WiFi network for screen mirroring performance is enhanced. Miracast reduces this dependence by making dual connections from the devices.

10. About Miracast

Miracast is a certification program of the WiFi Alliance based on their Wifi-Display specification. It defines a protocol to connect an external monitor or TV to a device, and therefore can roughly be described as "HDMI over WiFi", replacing the cable from the computer to the display.

It is peer-to-peer, and wireless, using a WiFi Direct connection. It allows sending up to 1080p HD video and 5.1 surround sound (AAC and AC3 are optional codecs, mandated codec is linear pulse-code modulation — 16 bits 48 kHz 2 channels). The connection is created via WPS and therefore is secured with WPA2. IPv4 is used on the internet layer. On the transport layer, TCP or UDP are used. On the application layer, the stream is initiated and controlled via RTSP, RTP for the data transfer.

At its most basic level, Miracast is a video streaming specification created by the WiFi Alliance. It allows a user to share whatever is displayed on their device's screen with another compatible product. The spec supports up to 1080p HD video. More specifically, Miracast is built on top of WiFi Direct, which allows devices to utilize WiFi to communicate with each other directly, instead of having to hop on a mutual wireless router.

Miracast devices negotiate settings for each connection, which simplifies the process for the users. In particular, it obviates having to worry about format or codec details. Miracast is "effectively a wireless HDMI cable, copying everything from one screen to another using the H.264 codec and its own digital rights management (DRM) layer emulating the HDMI system.

11. Difference between Miracast and AirPlay

The main difference is that, unlike Apple's mirroring standard which is proprietary, Miracast is open so that any platform or device manufacturer could embed and support it. As of right now, there are a number of major players who are willing to work on this including Intel, Microsoft, Realtek, AMD, Broadcom, Ralink, NVIDIA, TI, Qualcomm, Marvell, MediaTek, and the Android platform.

The second key difference that was mentioned before is the support of WiFi Direct by Miracast which reduces it dependence on the WiFi network as well as provides the BYOD's the ability to have a simultaneous and concurrent Internet connection while the Screen Mirroring function is live.

WiFi Direct doesn't need a wireless access point

WiFi Direct devices can connect to each other without having to go through an access point, that is to say you don't need to use your router.

This is because WiFi Direct devices establish their own ad-hoc networks as and when required, letting you see which devices are available and choose which one you want to connect to.

WiFi Direct is an official standard

It comes via the WiFi Alliance, the global industry association in charge of certifying WiFi kits. This means that you can be sure that any WiFi Direct enabled technology has been set to work with all the others without the need for special hardware.

WiFi Direct uses WPA2 Setup

WiFi Direct uses WPA2 to prevent unauthorised connections thus keeping your communications private.

12. Abbreviations and Terms

Please refer to this table for the definition of abbreviations and terms used in this document.

Abbreviation/Term	Definition
3G Network	Third generation (3G) network of mobile communications technology
4G LTE	4G Long Term Evolution; is the fourth generation of mobile telecommunications technology, succeeding 3G and preceding 5G.
AirPlay	AirPlay is a proprietary protocol stack/suite developed by Apple Inc. that allows wireless streaming between devices of audio, video, device screens, and photos, together with related metadata.
AP	Access Point; a hardware device or a computer's software that acts as a communication hub for users of a wireless device to connect to a wired LAN. APs are important for providing heightened wireless security and for extending the physical range of service a wireless user has access to.
BYOD	Bring Your Own Device; a practice using personal computing devices (ex.laptop, smartphone, tablets) in the workplace, network or education system
DLNA	Digital Living Network Alliance; an industry-wide standard for sharing data over a network.
DRM	Digital Rights Management
Ethernet	Family of computer networking technologies widely used for LAN
HDMI	High-Definition Multimedia Interface; HDMI is a digital interface whose purpose is to permit the transmission of audio and video signals through a single cable, while supporting faster data rates than its normal counterparts
Honeypot	In computer terminology, a honeypot is a trap set to detect, deflect, or, in some manner, counteract attempts at unauthorized use of information systems. Generally, a honeypot consists of a computer, data, or a network site that appears to be part of a network, but is actually isolated and monitored, and which seems to contain information or a resource of value to attackers.

Abbreviation/Term	Definition
Intel WIDI	Wireless Display (WiDi) technology, developed by Intel, enables users to stream music, movies, photos, videos and apps wirelessly from a compatible computer to a compatible HDTV or through the use of an adapter with other HDTVs. Intel WiDi supports HD 1080p video quality, 5.1 surround sound, and low latency for interacting with applications that are sent to the TV from a PC.
IP Address	Internet Protocol address (IP address) is a unique number consisting of 4 parts separated by dots, e.g. 165.113.245.3 Every machine that is on the Internet has a unique IP number.
LAN	Local Area Network;A network of interconnected workstations sharing the resources of a single processor or server within a relatively small geographic area. Typically, this might be within the area of a small office building.
MAC Address	Media Access Control Address; A MAC address is a hardware identification number that uniquely identifies each device on a network. The MAC address is manufactured into every network card, such as an Ethernet card or WiFi card, and therefore cannot be changed.
mDNS	Multicast Domain Name System; resolves host names to IP addresses within small networks that do not include a local name server. It is a zero configuration service, using essentially the same programming interfaces, packet formats and operating semantics as the unicast Domain Name System (DNS). While it is designed to be stand-alone capable, it can work in concert with unicast DNS servers.
Miracast	Miracast is a certification program of the WiFi Alliance based on their WiFi-Display specification. It defines a protocol to connect an external monitor or TV to a device, and therefore can roughly be described as "HDMI over Wifi", replacing the cable from the computer to the display.It is peer-to-peer, and wireless, using a WiFi Direct connection.
Peer-to-peer (P2P)	In a P2P network, the "peers" are computer systems which are connected to each other via the Internet. Files can be shared directly between systems on the network without the need of a central server.
PSK	phase shift keying;phase modulation that uses discrete changes of phase.
RS-232	RS-232 is a standard for serial communication transmission of data for computers; used for connections to computer peripherals such as control systems.
RTP	Real-Time Transport Protocol;an end-to-end network-transport protocol suitable for applications transmitting real-time data (such as audio, video, or simulation data) over multicast or unicast network services.

Abbreviation/Term	Definition
RTSP	Real Time Streaming Protocol;RTSP is an official Internet standard (RFC 2326) for delivering and receiving streams of data such as audio and video. The standard allows for both real-time ("live") streams of data and streams from stored data.
SSID	Service Set identifier;Identifies a network consisting of one or more access points. Such a network is also known as an Extended Service Set (ESS).
TCP	Transmission Control Protocol;A connection-oriented protocol that transmits data in byte streams. Data is transmitted in packets called TCP segments, which contain TCP headers and data.
TCP/IP	"Transmission Control/Internet Protocol;this is used for communications across interconnected networks and is being increasingly deployed to connect diverse computer architectures and platforms, both between enterprises and within enterprises. TCP operates at Layer 4 (the transport layer) of the OSI stack. IP operates at Layer 3 (the network layer) of the OSI stack. "
UDP	User Datagram Protocol; is part of the TCP/IP suite of protocols used for data transferring. UDP is a known as a "stateless" protocol, meaning it doesn't acknowledge that the packets being sent have been received. For this reason, the UDP protocol is typically used for streaming media. While you might see skips in video or hear some fuzz in audio clips, UDP transmission prevents the playback from stopping completely.
Virtual AP	Virtual Access Point;a secondary Wi-Fi hotspot created within a physical access point (AP).
VLAN	"Virtual Local-Area Network;a set of systems that, regardless of higher-layer addressing or location, is designated as a logical LAN and treated as a set of contiguous systems on a single LAN segment. VLANs can be proprietary or standardized using the IEEE 802.1q specification. "
WAN	Wide-area Network;used to distinguish the broader telecommunication structure from a local area network (LAN). A wide area network may be composed entirely of private structures, but the term seems to also connote the inclusion of public networks and all kinds of transmission media.
WiFi Direct	Initially called WiFi P2P, is a WiFi standard enabling devices to easily connect with each other without requiring a wireless access point. It is usable for everything from internet browsing to file transfer,and to communicate with more than one device simultaneously at typical Wi-Fi speeds.

Abbreviation/Term	Definition
WiFi	Wireless Fidelity;refers to wireless network components that are based on one of the Wi-Fi Alliance's 802.11 standards.
WLC	Wireless LAN Controller
WPA	WiFi Protected Access;WPA is a security protocol designed to create secure WiFi networks. It is similar to the WEP protocol, but offers improvements in the way it handles security keys and the way users are authorized.
WPS	WiFi Protected Setup (originally Wi-Fi Simple Config) is a network security standard that attempts to allow users to easily secure a wireless home network but could fall to brute-force attacks if one or more of the network's access points do not guard against the attack.

Arrive CarePoint Foundation Software Support Services

Thank You for choosing us to serve you. Your suggestions for Arrive AirPoint® are welcome.

To make a technical support request, please contact ARRIVE Technical Support (netsupport@arrivesys.com).

The product warranty related to AirPoint enabled devices can be found at http://www.arrivesys.com/warranty.

Additional Resources

Our goal is to ensure that our customers receive exceptional service from the best resource available to answer questions quickly and accurately. We work to resolve our customers' product-specific questions and concerns however, when customers are experiencing issues outside the scope of ARRIVE products, we will refer customers to the appropriate resource who is best equipped to assist with those issues. These resources may be the customer's internal personnel, an ARRIVE-authorized business partner, a certified consultant, or a third-party provider. ARRIVE Professional Services and ARRIVE Academy teams also offer a wide variety of services.

Topics that are not covered under an Arrive CarePoint program, where an ARRIVE Customer Support team member will proactively provide the most appropriate alternative resource, include:

Training-ARRIVE Academy is the best resource for training, offering classroom training, real-time Learning, custom training, self-study guides, and an annual customer conference. Visit ARRIVE Academy to search and register for courses and products, monitor your learning progress through training tracks, and join online communities with product experts and other customers.

- Performing software, product, application, or job-related activities, such as software installation, data entry, creating reports, etc.*
- Assisting with third-party software (installation, training, trouble-shooting, integration, etc.).
- Providing organization-specific consulting or consulting advice.
- Repairing data or database issues caused by user error or third-party software.

Refer to the CFSS coverage information at http://carepoint.arrivesys.com/cfss for additional information and resources.

Note: *References in this document to third-party software, products or applications, does not encompass all third-party software, products and applications that ARRIVE provides (directly or through an authorized ARRIVE Business Partner) as part of a customer's solution.

www.arrivesys.com

Arrive Systems, Inc.
Toll Free: +1-844-427-7483 (USA / Canada)

Email: info@arrivesys.com