wePresent

WiPG/WiCS Devices

Network Deployment User Guide

For more information
www.wePresentWiFi.com

Sales: sales@wePresentWiFi.com
Support: help@wePresentWiFi.com

NETWORK DEPLOYMENT USER GUIDE

wePresent

Contents

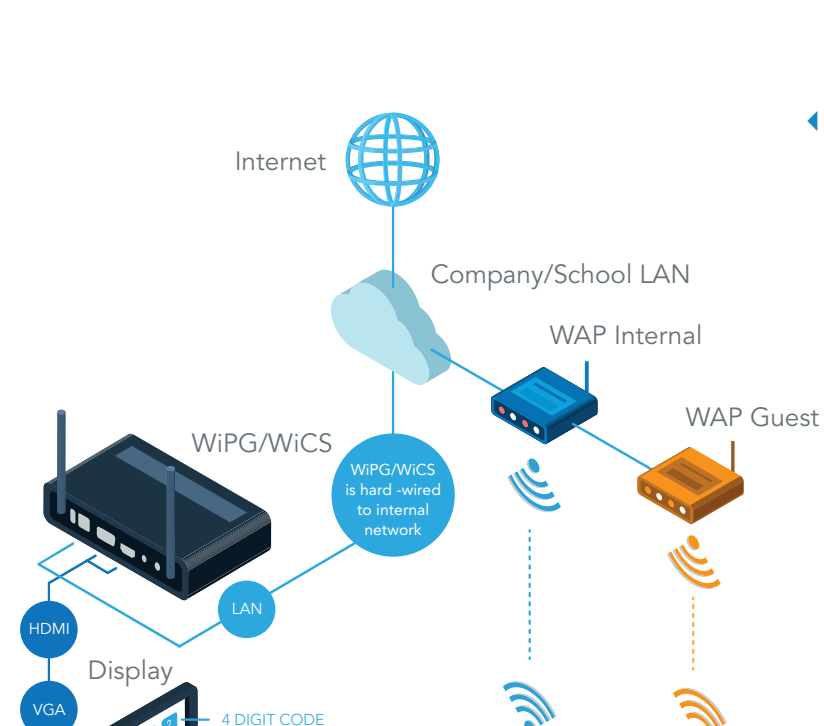
wePresent

1 Introduction

The **wePresent WiPG/WiCS devices** help users to bridge the technology gap, allowing businesses and classes to enjoy the benefits of wireless presentation.

When connected to a display or projector, users can mirror their content without the need for connecting cables. The WiPG/WiCS products can be used as stand-alone devices, generating their own Wi-Fi signal or connected to a network through the LAN Ethernet port.

Windows and macOS users can share their desktop by installing and running free software called MirrorOp (Sender). The MirrorOp software is available from the wePresent website and WiPG/WiCS admin panel. Android and iOS users can share their content by installing the free MirrorOp (Presenter) application available from Google Play and the App Store.



Basic WiPG/WiCS deployment example

The wePresent WiPG/WiCS devices are designed for commercial implementation in corporate, education, government, healthcare and public environments. This documentation provides deployment information for three current wePresent models (WiPG-1000, WiPG-1600w and WiCS-2100 & WiPG-2000).

For more information, please visit our website http://wepresentwifi.com or email our help team at help@wepresentwifi.com.

wePresent

2 User Experience

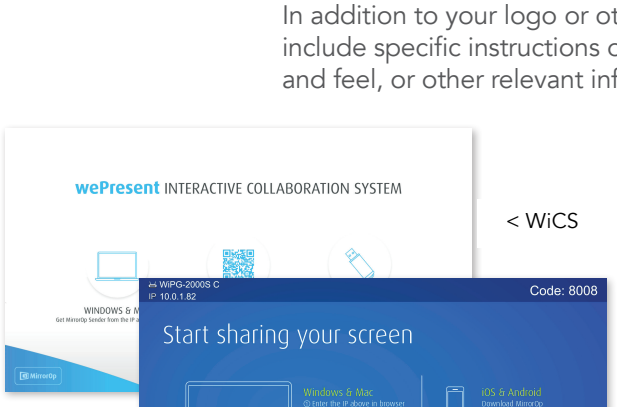
2.1 Standby Screen Display

The WiPG/WiCS devices show the standby screen when the connected display/ projector is turned on. Elements shown on the standby screen include the hostname, SSID, IP address, software download instructions and 4-digit security code (login code/passcode). The display can be personalized to allow custom login code and branding.

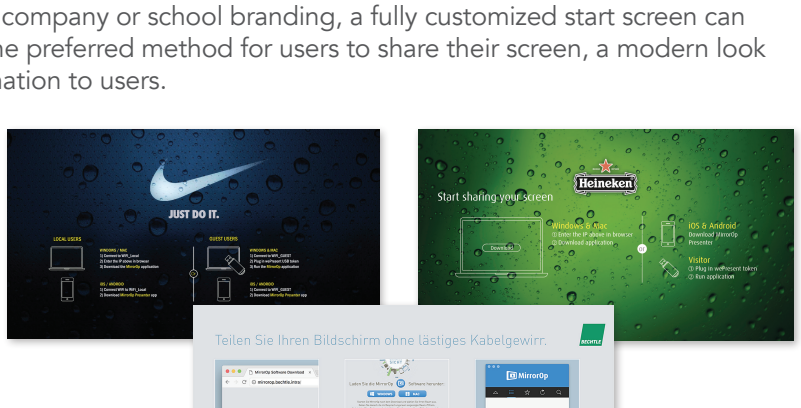
Customize your Start Up Display

Integrating your brand into your wireless presentation solution is an effective way to reinforce your organization's focus on wireless interaction and collaboration to your audience.

In addition to your logo or other company or school branding, a fully customized start screen can include specific instructions on the preferred method for users to share their screen, a modern look and feel, or other relevant information to users.



Default wePresent Display



Customize Visual Identity and provide clear User Instructions

Hostname & SSID

The hostname and SSID can be customized / renamed so that users can easily identify and log into the correct device if multiple units have been deployed on the network.

IP Address

Each WiPG/WiCS device will be assigned an IP address. By typing the IP address in a web browser, users will have access to software download, admin panel, control panel, and WebSlides for that particular device.

4-Digit Security Code

The security code prevents people outside the conference room/classroom from being able to log into the presentation.

There are three settings of operation for the security login:

1) Random: a new 4-digit code is generated after the last user disconnects.
2) Fixed: a static 4-digit code can be set from the admin panel.
3) Disabled: 4-digit security code can be disabled through the admin panel.

wePresent

3 WiPG/WiCS Device Installation

To Present content to a wePresent, users will need to first make a connection. Users can either connect to the wePresent's own Wi-Fi signal, or when wePresent is network-connected, through the local (wireless) network infrastructure.

3.1 Stand-Alone Connection Mode

No ethernet connection, own Wi-Fi signal on

Most wePresent models are able to broadcast their own Wi-Fi signal, becoming an access point/ hotspot that users can log on to present. Our range of models offers different broadcast options, ranging between 2.4 GHz and 5 GHz (ac). All wePresent models that have ability to produce Wi-Fi, can be used as stand-alone units, creating a secure wireless presentation environment. All wePresent models support various levels of data encryption, ensuring your content is shared safely and secure.

NOTE: Wi-Fi interference can cause of lag during a presentation. To ensure optimal conditions for wireless presentation, always make sure that wePresent's Wi-Fi channel is correctly separated from other Wi-Fi activity, and that Wireless Access Points are not obstructed, or too far away.

Stand-Alone Connection Mode Basic Diagram

Recommended Enviroment

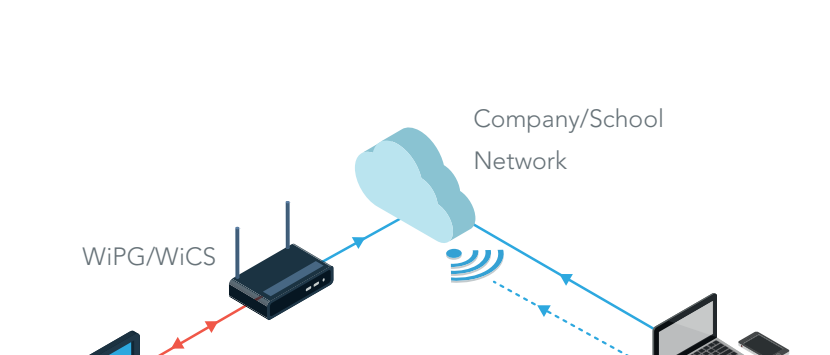
Small to medium size room with clear Wi-Fi having no more than 5 other access points.

3.2 Network Connection Mode (Option A)

Ethernet connected, own Wi-Fi signal off

The WiPG/WiCS device is able to connect to the local enterprise/school network via the Ethernet/LAN port located in the back of the device using an Ethernet cable. In the network connection mode Option A, the Wi-Fi signal of the WiPG/WiCS device will be disabled. Both guest and internal users will access the WiPG/WiCS device through the access point (AP) on the enterprise/school network.

In this setup, all traffic and wireless security is in the hands of the existing network.



Network Connection Mode (Option A) Basic Diagram

Recommended Enviroment

Office or school with many access points currently installed. Network connection mode Option A is a good option in environments where more than 10 WiPG/WiCS units are closely deployed. This option is ideal for networks that do not allow additional Wi-Fi APs due to security concerns.

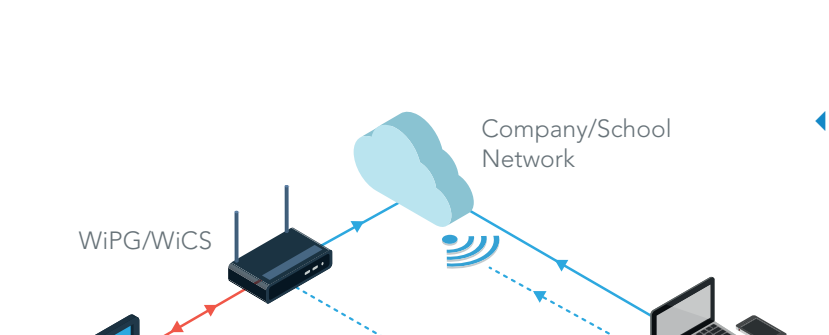
3.3 Network Connection Mode (Option B)

Ethernet connected, own Wi-Fi signal on

wePresent can be connected to a network via the Ethernet/LAN port located in the back of the wePresent. In network connection mode Option B, the wePresent will continue to broadcast a Wi-Fi signal which acts as a wireless access point (WAP).

The gatekeeper feature can be used to restrict WAP connectivity allowing the WAP to act as an additional network access point, or as an alternative (restricted) access point for guests.

This scenario allows guest users to connect to the wePresent's in-room Wi-Fi signal, while internal users connect over the corporate (wireless) infrastructure.



Network Connection Mode (Option B) Basic Diagram

Recommended Enviroment

Office or school with many access points currently installed. Network connection mode Option B is a good option in environments where more than 10 WiPG/WiCS units are closely deployed. Also ideal for scenarios where no corporate Wi-Fi AP exists or the corporate Wi-Fi is not open to guest users.

NOTE: If wePresent is broadcasting its own Wi-Fi signal, the Gatekeeper security feature allows to customize network connectivity over wePresent's Wi-Fi signal. You can restrict network access – allow all / block all / internet only – according to network's security level.

3.4 Network Connection Mode (Option C)

Ethernet connected, own Wi-Fi signal off

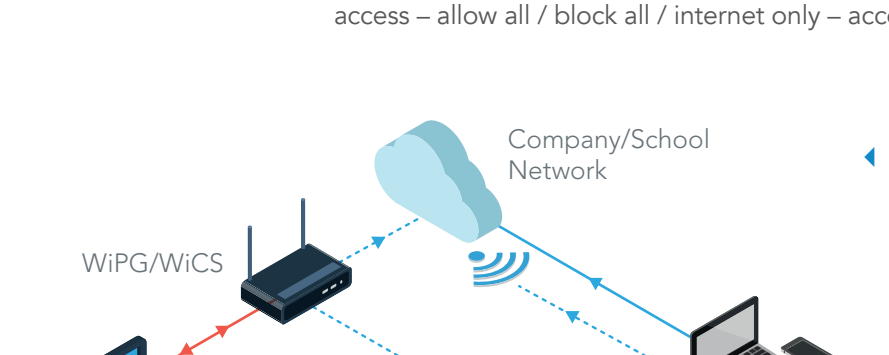
Your wePresent is able to connect wirelessly to the local enterprise network using Wi-Fi. Depending on your wePresent model, it can connect over 2.4GHz, or 5GHz. To do this, set your wePresent to Wi-Fi Station Mode in the ADMIN Panel. Once configured, both guest and internal users can access the wePresent through the network enterprise's access point.

Network Connection Mode (Option D)

Network connected as Wi-Fi Station, own Wi-Fi signal on

Alternatively you can set wePresent to Station & AP Mode. This will make your wePresent behave as a repeating Access Point to the network enterprise's access point. It is still possible to manipulate the wireless settings to make wePresent broadcast a unique SSID, channel etc.

NOTE: If wePresent is broadcasting its own Wi-Fi signal, the Gatekeeper security feature allows to customize network connectivity over wePresent's Wi-Fi signal. You can restrict network access – allow all / block all / internet only – according to network's security level.



Network Connection Mode (Option C & D) Basic Diagram

Recommended Enviroment

Office or school with many access points currently installed. Also an option when corporate network consists of segregated VLAN's. This option is ideal when network policies do not allow additional Wi-Fi AP's and Ethernet connection is not available. Additionally, if wePresent is on a movable AV cart, it can still be network connected while it is mobile.

NOTE: In above scenario's, performance may not be optimal due to two Air Hops between User and wePresent.

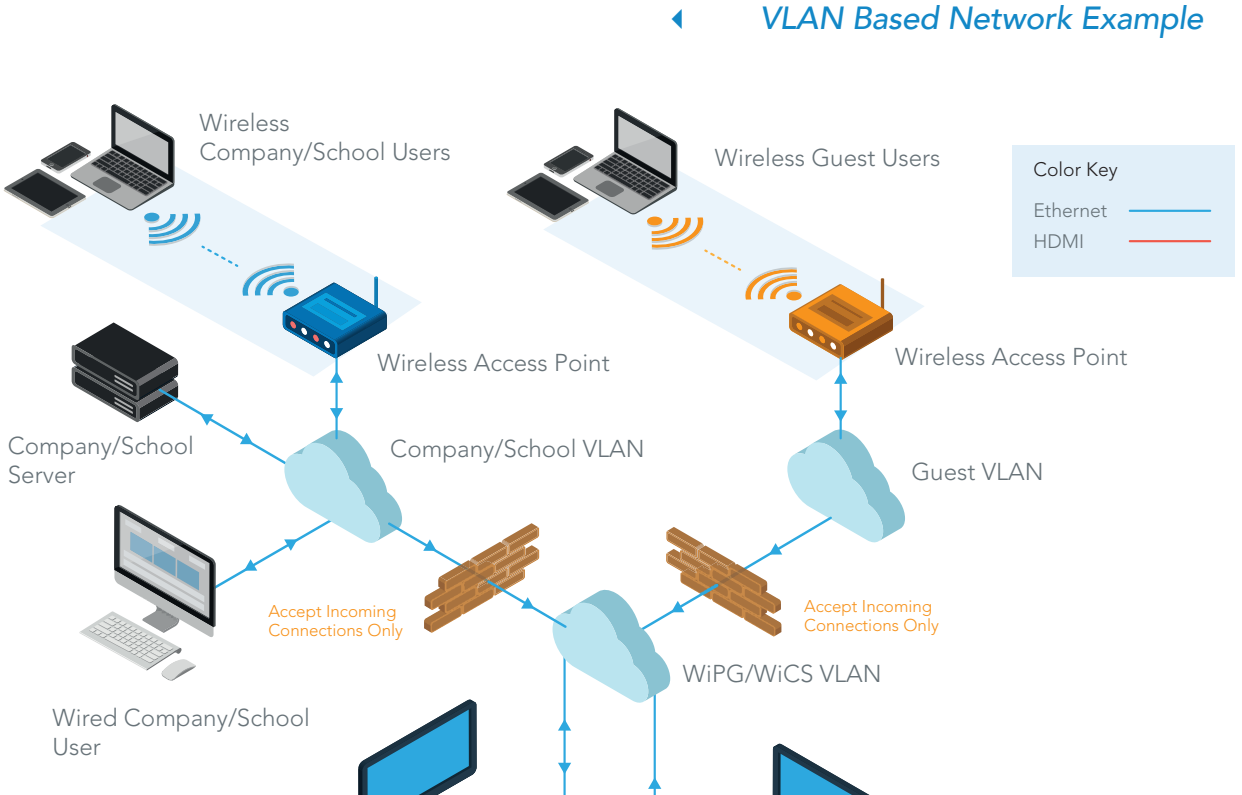
3.5 Deployment Options for Guest Network Access

In conference rooms, classrooms or meeting rooms, network managers need to be able to accommodate both internal and guest users and their respective network privileges. The standard network practice is to have a separate network for guest users to access, either a VLAN-based network or a physical air-gap network.

3.6 VLAN Based Network (Option D)

Virtual LANs (VLANs) are partitions that network administrators have set to provide separate networks for internal users and guest users in order to match different security requirements. The VLAN deployment diagram shows how the WiPG/WiCS devices communicate with the internal VLAN and guest VLAN.

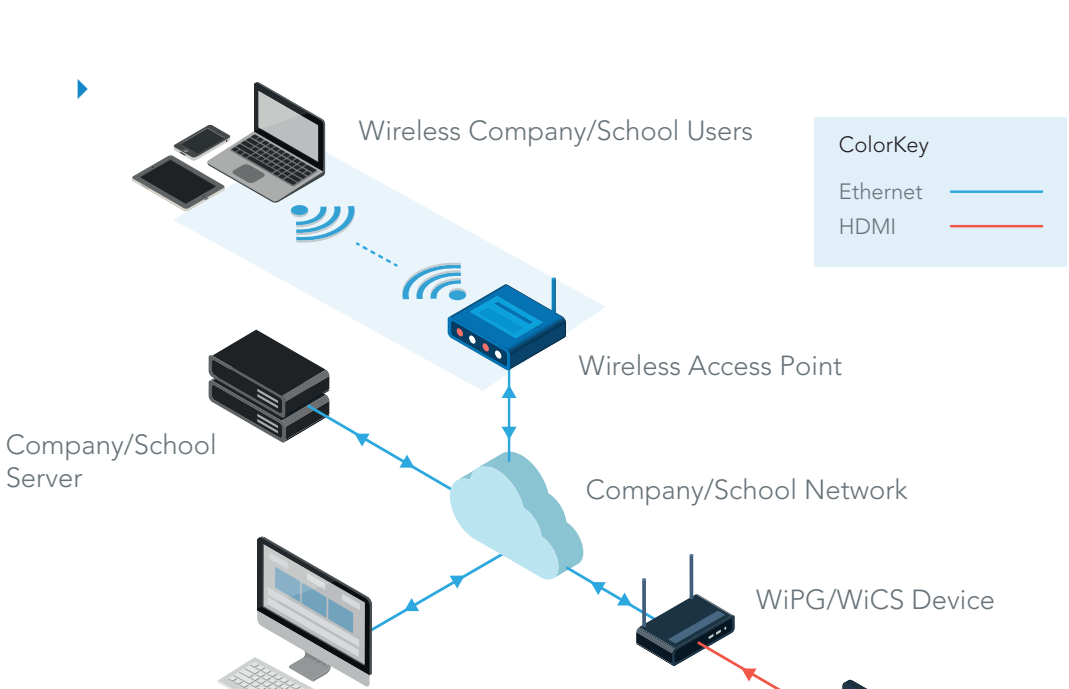
VLAN Based Network Example



3.7 Data Transport

The WiPG/WiCS device employs a proprietary protocol to transport the screen data from a computer or smart mobile unit to the WiPG/WiCS device. The data is encrypted and users accessing the data will need the four-digit code shown on the display/projector when launching the MirrorOp software.

WiPG / WiCS Data Transport



4 Connecting to WiPG/WiCS Device

4.1 Connecting Computers

Frequent Users - Software installation (advised)

MirrorOp Installation

For regular users presenting from Windows or Mac, it's recommended to install the MirrorOp software, (but not required). MirrorOp software installation can be downloaded from wepresentwifi.com, or from your device's Admin Panel.

There are no additional licensing fees for multiple software installations across the enterprise.

Guest Users - No software installation

Download & Show

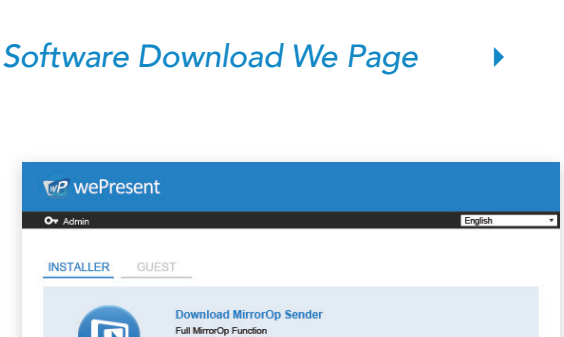
For guest users it is easiest to download and run a MirrorOp executable file. This file allows users to launch MirrorOp and connect to one target wePresent, without need to install the software. The MirrorOp executable file is available on each wePresent's Admin Panel (or can be gathered and offered from an alternate location).

USB Plug & Show

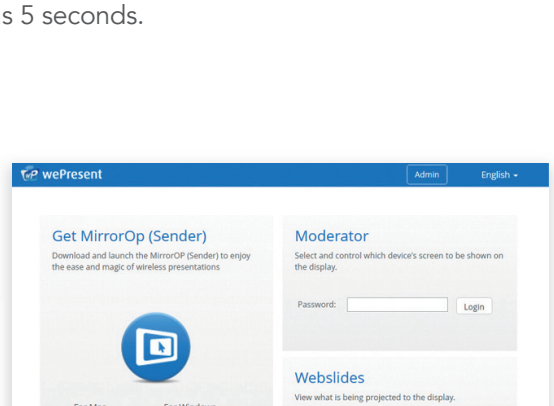
Customizable Plug & Show USB tokens can be created for each individual wePresent unit. These will works the same as the MirrorOp executable file, but the file is accessed via USB instead of downlaoding.

NOTE: Download & Show and USB Plug & Show are the quickest way to allo guest users to target wePresent without software installation in as few as 5 seconds.

Software Download We Page ▸



(WiPG)



(WiCS)

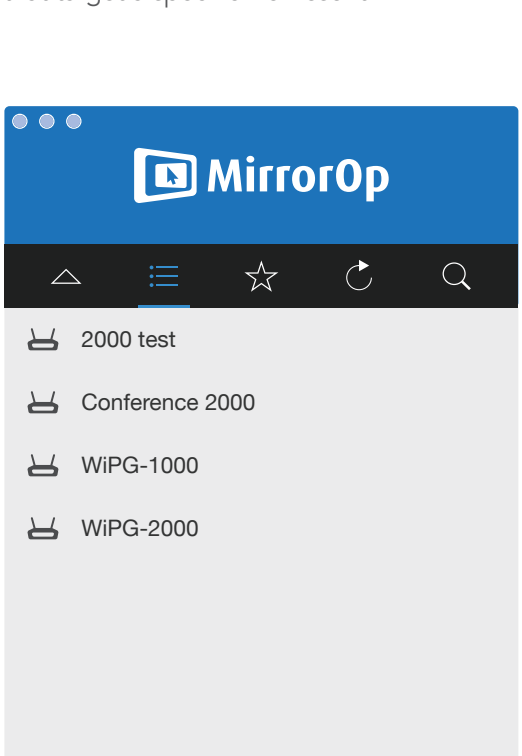
4.2 Detect wePresents

MirrorOp Device Discovery Scan

The MirrorOp software will by default perform a 'Device Discovery Scan' at startup. This Device Discovery is a 'UDP broadcast', which generally won't traverse network segments, therefore it will only detect wePresents in the VLAN where the user is situated in.

Due to network segmentation, it may sometimes be better to avoid this Device Discovery Scan and instead 'target a specific wePresent'. Targetting a wePresent is especially useful when working within a segemented network. The most obvious ways of targetting one wePresent is of course Manual Entry of either the IP address or Hostname, as described below.

Since Manual Entry may be considered cumbersome in some situations, we have other options that target a specific wePresent.



MirrorOp Device Discovery Screen

Device (SSID) Listing

To view a current listing of connected WiPG/WiCS devices, click on the refresh icon from the menu on computers or drag down the window on mobile devices.

Manual Entry

The WiPG/WiCS device allows users to manually enter the hostname or IP address of the device in order to locate the device. The hostname or IP address can be entered in the "Input hostname or IP" field located at the bottom of Device Discovery Screen on computers. On mobile devices, IP address or hostname can be entered in the search field.

4.3 Target a single wePresent

Use one of the 'Direct IP Methods'

When users are located in a restricted network segment (VLAN), MirrorOp will not detect wePresent units located in other network segments. Users that are connecting from a different VLAN, or users that simply want to connect to a certain wePresent, can use our Direct IP Methods to target a wePresent:

- Manual Input IP, or Hostname
- Guest Executable file - see page 12
- Plug & Show USB - see page 12
- Device Profile (.mop) - see page 12
- Favorites
- PresentSense

The methods listed below are IP-bound allowing a straight connection to a single target wePresent. These methods don't reply on a Device Discovery scan allowing them to traverse a segmented network. In order to communicate to a wePresent, any firewall settings must allow port communication between the use;'s and the targeted wePresent's IP address.

Make Device Discovery traverse VLAN's

Device Discovery is designed to limit unwanted activity over the entire network, however, it can be manipulated to work over multiple VLAN'sthrough alternative ways. Modifying Device Discovery should only be attmpted by qualified IT professionals.

Forward UDP Broadcast
The Device Discovery protocol uses a standard UDP broadcast. Network switches can be configured to forward these broadcasts to the wePresent's network segment.

VLAN Tagging
'VLAN tagging' can allow Device Discovery locate wePresents in other network segments. Correctly configured VLAN tagging will allow Device Discovery to detect wePresents located in other 'stacked VLAN's'.

4.4 MirrorOp Software Development

Listed below are a few options for software deployments.

Guest Executable File

Users or the IT department can install the full MirrorOp (Sender) software directly from the admin panel/web page of the WiPG/WiCS device. The option to download the quick executable application (portable software) to launch MirrorOp is also available on the admin panel/web page.

Plug & Show USB

Click on the "Make PnS Token" icon on the standby screen to copy the MirrorOp (Sender) executable file (protable software) to the attached USB drive. (Guest) users can launch the MirrorOp executable file directly from the PnS token to connect to the target WiPG/WiCS device

Device Profile (.mop)

The WiPG/WiCS Device Profile (.mop) file provides a quick way to connect to a predefined wePresent. By defining the WiPG/WiCS Device Profile, a user can double click on the file and it will connect his MirrorOp software to the predefined WiPG/WiCS device automatically. In order for the .mop file to recognized by your Operating System, the MirrorOp software needs to be installed!

From the wePresent's IP based admin panel you can download the Device Profile (.mop). Y The .mop file is a basic XML text file with the following template:

```
<?xml version="1.0" encoding="utf-8"?>
<Devices>
        <MirrorOp>
                <Device>
                        <Name>USERNAME</Name>
                        <Device_name>DEVICENAME</Device_name>
                        <IP>192.168.100.10</IP>
                        <LoginCode>1234</LoginCode>
                </Device>
        </MirrorOp>
</Devices>
```

NOTE: IT professionals can easily manipulate variables in the XML file to create additional .mop files for other units.

4 Connecting to WiPG/WiCS Device

MSI Install

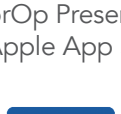
Using MSI Installer, the enterprise IT department can deploy the MirrorOp software to users' Windows laptops directly from the MSI command line.

Mobile Devices Connection

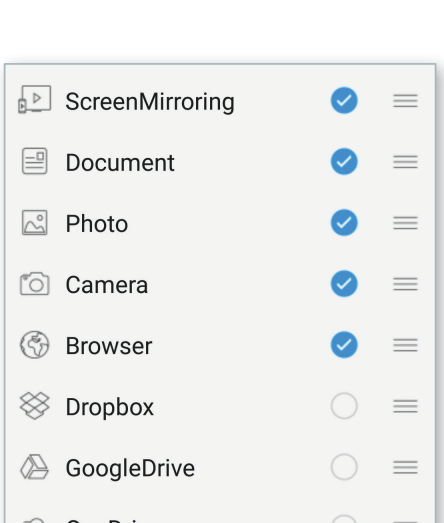
Smartphones and Tablets

When presenting from an iOS or Android device (both smartphone and/or tablet), users will need to install the MirrorOp Presenter App.

MirrorOp Presenter can be downloaded for free from the Apple App Store or Google Play Store.



MirrorOp Presenter app



Native Mirroring - Apple Airplay & Google ChromeCast

Airplay
wePresent can provide basic or advanced Apple AirPlay mirroring based on the unit's model. For users to content and present using Apple AirPlay select the model from the availabl device list. Both the presenter's device and wePresent must be able to make a wireless network connection.

Google ChromeCast
Collaboration series wePresent models (WiCS) provide native mirroring from Google Chromecast using the feature built into Chrome OS computers and via the Google Home app. For users to content and present using Google Chromecast, select the model from the availabl device list. Both the presenter's device and wePresent must be able to make a wireless network connection.

5 WiPG/WiCS Customization

Domain Name Service

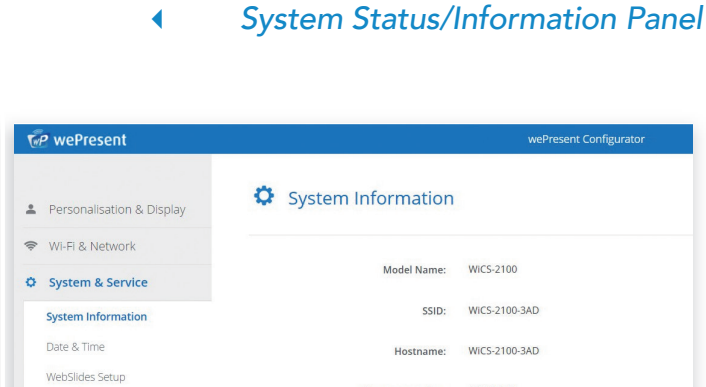
DNS - Hostname
An common way to connect to a target wePresent is to manually input the wePresent's IP address. Because inputting an IP address can be confusing for some users, it is possible to register a Hostname for each wePresent IP address within your network domain (DNS). This allows users to input the wePresents HostName in MirrorOp, instead of the IP address.

5.1 Admin Panel

The WiPG/WiCS device can be customized and configured through the built-in web pages of the device called the "admin panel". Parameters such as device IP address, WebSlides settings, centralized management, and WiPG/WiCS connected (display) devices are set under the admin menu option. The default password is admin, which can be changed.

System Status/Information Panel

(WiPG)



(WiCS)

5.2 Firewall Settings

The MirrorOp software communicates with the target WiPG/WiCS device passing through network security systems such as firewalls. A set of rules need to be established so that traffic can be filtered and passed through the firewall. The firewall administrator will be prompted by the operating system to add a rule if a rule does not exist.

Port Table: The firewall administrator can allow or restrict certain data to be communicated from the user to the WiPG/WiCS device using the port table.

5.3 Port Table (WiPG-1000 / 1600w):

	USAGE	DIRECTION	PORT#	NOTE
TCP	**Command**	Both	443 3268 389	Air play also uses this port.
	Data	Both	8080 31865 515	
	Audio	Both	1688	Used for screen projection and audio data transfer; need to open it to let audio projection work.
	Video	Both	1041	
	UoIP	Both	3240 6000	
	DLNA	Both	2869 49152 49153	DLNA CMD port for connection created.
	Airplay		80 3689 7000 49153	
UDP	**Airplay**	Both	5353	
	Device Discovery	Inbound	1047 1048 1049	Used for device discovery to find available devices; suggest opening all these 3 ports (1047~1049), and otherwise application can't find devices; may need to enter IP/hostname manually.
	NetBIOS Name Service	Both	137	Standard port number. This if for hostname used with windows.
	SNMP	Both	161	Standard port number. This is SNMP protocol port number.
	DLNA	Both	1900 50000- 65500	SSDP broadcast used. DLNA will select one of these ranges to do user action.
TCP/ UDP	**Airplay**		554	

5.3 Port Table (WiCS - 2100):

	USAGE	PORT#
TCP	**MirrorOp Projection**	1234
	AirPlay & Google Cast	8008 8009 38351 47000 7000 7100
	UoIP	3240 6000
	Web Page	7020 80 443
	Rest API	4001
	DNS	53
UDP	**Devices Discovery**	37994 5353
	AirPlay Discovery	45690
	NetBIOS Name Service	137 138
	MirrorOp Projection	54022
	DNS	53
	DHCP	67

5.4 Wi-Fi Protocol

WiPG/WiCS devices have both 2.4G and 5G Wi-Fi capability. Actual performance might vary due to radio-frequency (RF) interference. For small-scale deployment, a Wi-Fi channel analysis tool to find the proper available channel for the WiPG/WiCS device is recommended. For large-scale deployment, consulting a professional Wi-Fi integrator, or utilizing the enterprise/school network's Wi-Fi via the Ethernet connection is recommended.

Channel Lists for the WiPG/WiCS device:

2.4G BAND

CHANNEL	FREQUENCY (MHZ)	EU*	WW
1	2412	Yes	Yes
2	2417	Yes	Yes
3	2422	Yes	Yes
4	2427	Yes	Yes
5	2432	Yes	Yes
6	2437	Yes	Yes
7	2442	Yes	Yes
8	2447	Yes	Yes
9	2452	Yes	Yes
10	2457	Yes	Yes
11	2462	Yes	Yes
12	2467	Yes	No
13	2472	Yes	No

*EN 300 328 V1.9.1. Regulation

5G BAND

CHANNEL	FREQUENCY (MHZ)	NA	EU*	JP	WW
36	5180	Yes	Yes	Yes	No
40	5200	Yes	Yes	Yes	No
44	5220	Yes	Yes	Yes	No
48	5240	Yes	Yes	Yes	No
149	5740	Yes	No	No	No
153	5765	Yes	No	No	No
157	5785	Yes	No	No	No
161	5805	Yes	No	No	No
165	5825	Yes	No	No	No

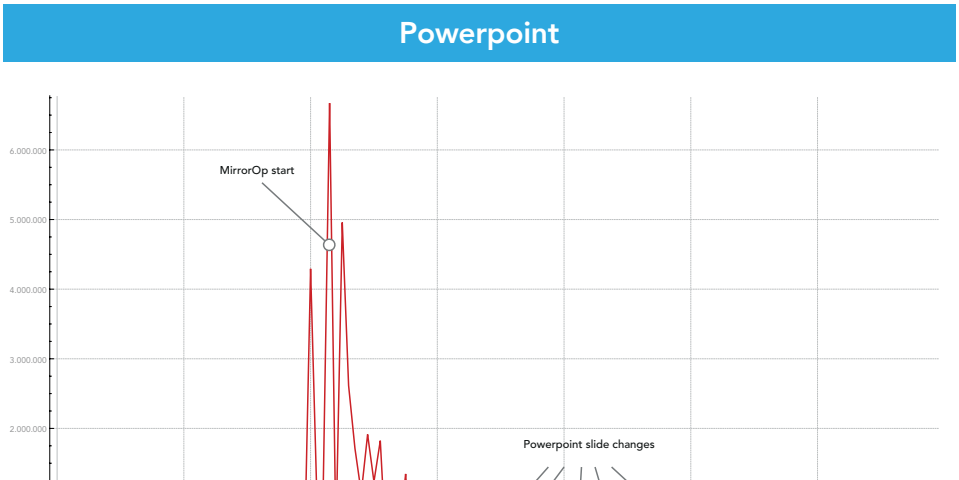
Adaptive Frequency Hopping of EN 300 328 V1.9.1 regulation requests the WiPG/WiCS device to implement the mechanism like Detect and Avoid (DAA) when an equipment identifying frequencies is being used by other devices. The Wi-Fi signal of the WiPG/WiCS device needs to be temporarily turned off if there is interference from different Wi-Fi access points or RF devices in the same environment.

5.5 Bandwidth Usage Scenario´s

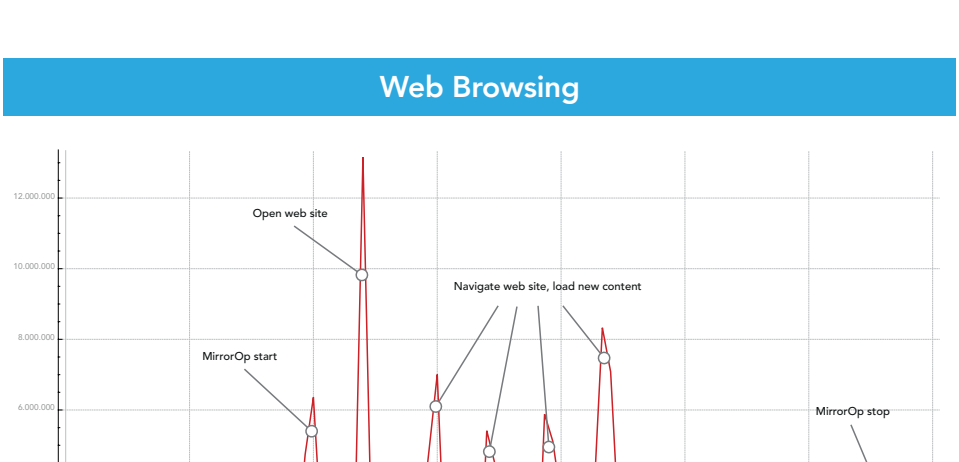
Bandwidth Allocation

It is common to limit bandwidth activity or to prioritize bandwidth usage for certain processes The diagrams below outline the bandwidth requirements for different types of presentations.

Powerpoint

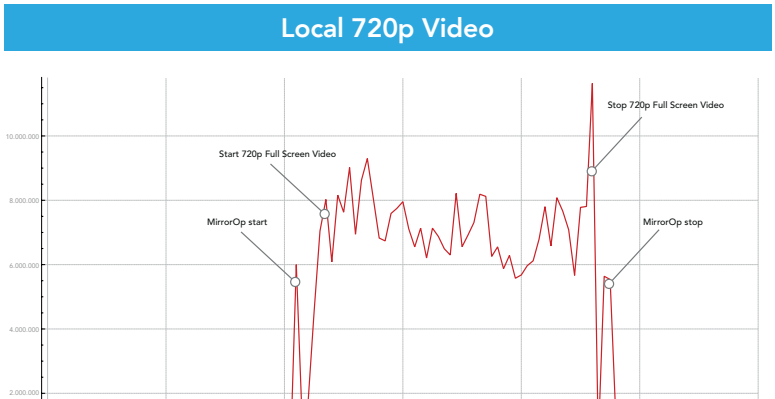


Web Browsing

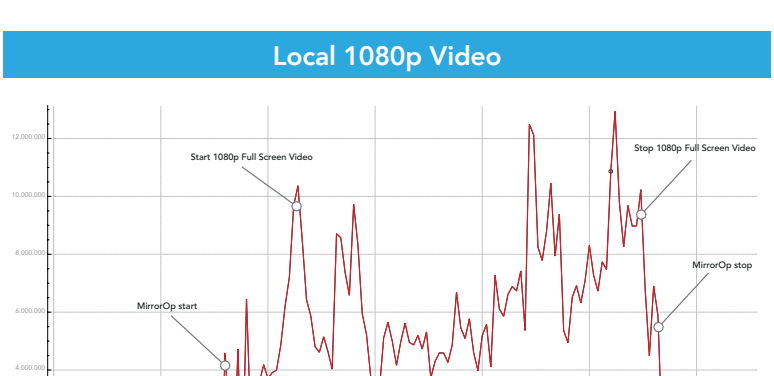


5 WiPG/WiCS Customization

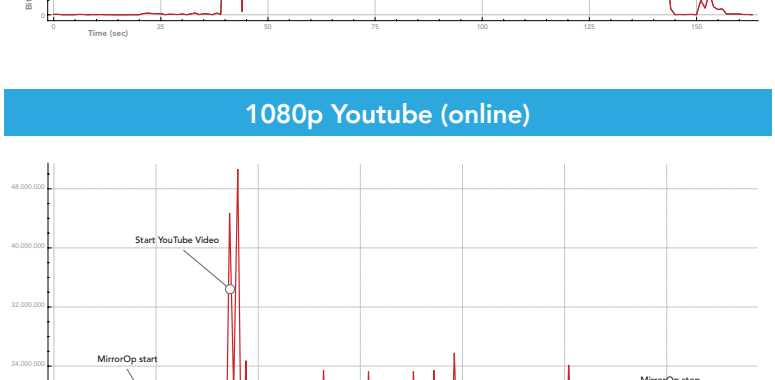
Local 720p Video



Local 1080p Video



1080p Youtube (online)



wePresent

6 WiPG/WiCS Device Secuirty

6.1 GuideWiPG/WiCS Device Security

Network security consists of different polices adopted to prevent and monitor unauthorized access, misuse, and/or modification of network resources. The WiPG/WiCS device has been designed to work in and adhere to a variety of computer network security environments: businesses, education, government and other public entities.

When the WiPG/WiCS device is connected to a corporate/school network, all traffic from the device is treated as from the corporate/school network. With the WiPG/WiCS WiFi disabled, the device sits on the network like any other network device (printer, etc.). It is important to remember that when connected to a corporate/school network, the WiPG/WiCS device is as secure as the standards set by the supporting network.

6.2 GuideWiPG/WiCS Secuirty Features

Enhanced security features are implemented in the WiPG/WiCS system to ensure the confidentiality, integrity and availability of the information communicated with the WiPG/WiCS system. (Table on next page)

MODULE/APPLICATION	SECURITY ENHANCEMENT	NOTE
MIRROROP		
Screen data	AES Encryption, 128-bit key Salsa20 Encryption	(WiPG-1000/1600w) (WiCS-2100)
Audio data	No encryption	(WiPG-1000/1600w, WiCS-2100)
Control data, command data	AES Encryption, 128-bit key Salsa20 Encryption	(WiPG-1000/1600w) (WiCS-2100)
WEB		
Web server	http (port 80), https (port 443)	Lighttpd (version: 1.4.4.1) OpenSSL (version: 1.0.2h)
Download	http (port 80) No encryption	
Conference control	https (port 443)	
Web management data	https (port 443)	
Web security assessment (WiPG-1000/1600w)	Patched	OWASP TOP 10 common Web Vulnerabilities
REMOTE MANAGEMENT		
SNMP (WiPG-1000/1600w)	SNMP v2 Protocol, SNMP v3 Protocol	(WiPG-1000) (WiPG-1600w)
CMGS (WiPG-1000/1600w, WiCS-2100)		Based on REST API
WIFI NETWORK		
WiFi	WEP, WPA, WPA2, WPA-Enterprise, WPA2-Enterprise.	(WiPG-1000/1600w, WiCS-2100) (WiPG-1000/1600w) (WiPG-1000/1600w)
WEPRESENT SYSTEM		
Firmware	MD5 encryption AES 256, RSA 4096	(WiPG-1000/1600w) (WiCS-2100)
Telnet, SSH	Disabled	
Port scan (WiPG-1000/1600w)	Done	
Vulnerability scan (WiPG-1000/1600w)	Patched	Nexpose.com
APPLICATION		
Windows	Digital signature	
Mac	Digital signature	

wePresent

7 Firmware Upgrades

7.1 Single Device (Web Interface)

The WiPG/WiCS device supports firmware upgrades via the web interface. The upgrade is deployed as a single file that is uploaded and programmed by the device. The firmware upgrade takes approximately 5 minutes to load.

7.2 Multiple Devices

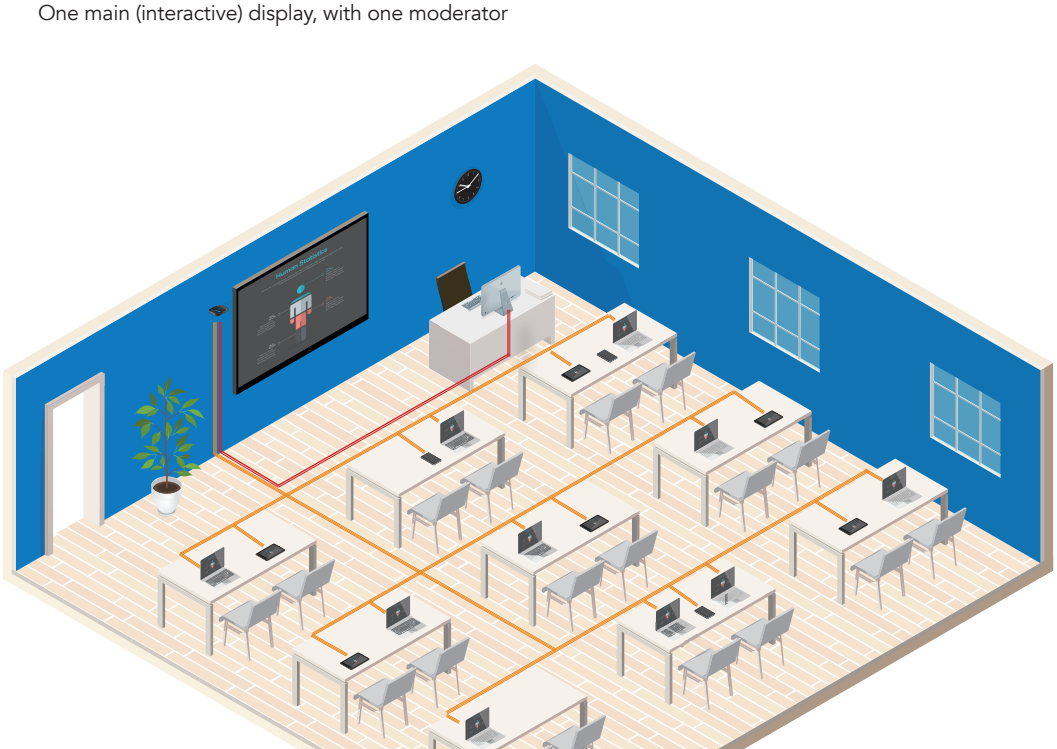
wePresent provides a management feature to upgrade multiple WiPG-1000/WiPG-1600w /WiCS-2100 devices remotely. Users can configure and start the FTP firmware upgrade via SNMP/REST API (CMGS) .

wePresent

8 Deployment Scenarios

8.1 Classroom with one wePresent

One main (interactive) display, with one moderator



Main Display

Presentation

- Present content from a device
- Instructors can use Moderator Control features to allow students to present content from their own device (up to 4 at a time).

Interaction (Touch Screen / USB Mouse)

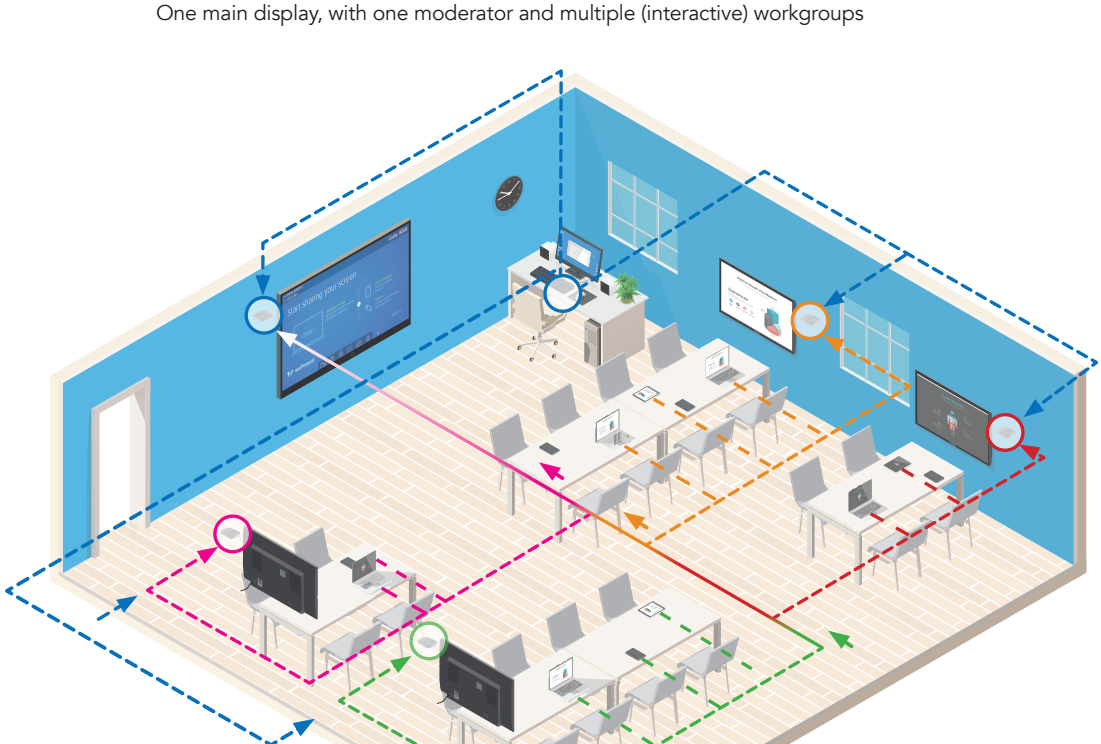
- Control any computers on the touch display, or with mouse.
- When content is projected, annotations can be made on top of the presentation.
- Write draw at any time on virtual whiteboard

Collaboration (WebSlides)

- With Webslides, content shown on wePresent can be viewed and saved by the class on their own device.

8.2 Classroom with multiple wePresents

One main display, with one moderator and multiple (interactive) workgroups



Workgroups

Presentation

- Students present content from their own device (up to 4 at a time).
- Or, present content from any other HDMI device with a SharePod.
- Content from one wePresent to other wePresent units.

Interaction (Touch Screen / USB Mouse)

- Control any computers on the touch display, or with mouse.
- When content is projected, annotations can be made on top of the presentation.
- Write draw at any time on virtual whiteboard

Collaboration (WebSlides)

- With Webslides, content shown on wePresent can be viewed and saved by the class on their own device.

8.3 Conference Room with one wePresent

One main (interactive) display, no moderator

Main Display

Presentation

- Present content from a device
- Allow multiple users can present contetn from their own device (up to 4 at a time).

Interaction (Touch Screen / USB Mouse)

- Control any computers on the touch display, or with mouse.
- When content is projected, annotations can be made on top of the presentation.
- Write draw at any time on virtual whiteboard

Collaboration (WebSlides)

- With Webslides, content shown on wePresent can be viewed and saved by conference particpants.