WDC10/20
InstaShow™ Series
Security White Paper

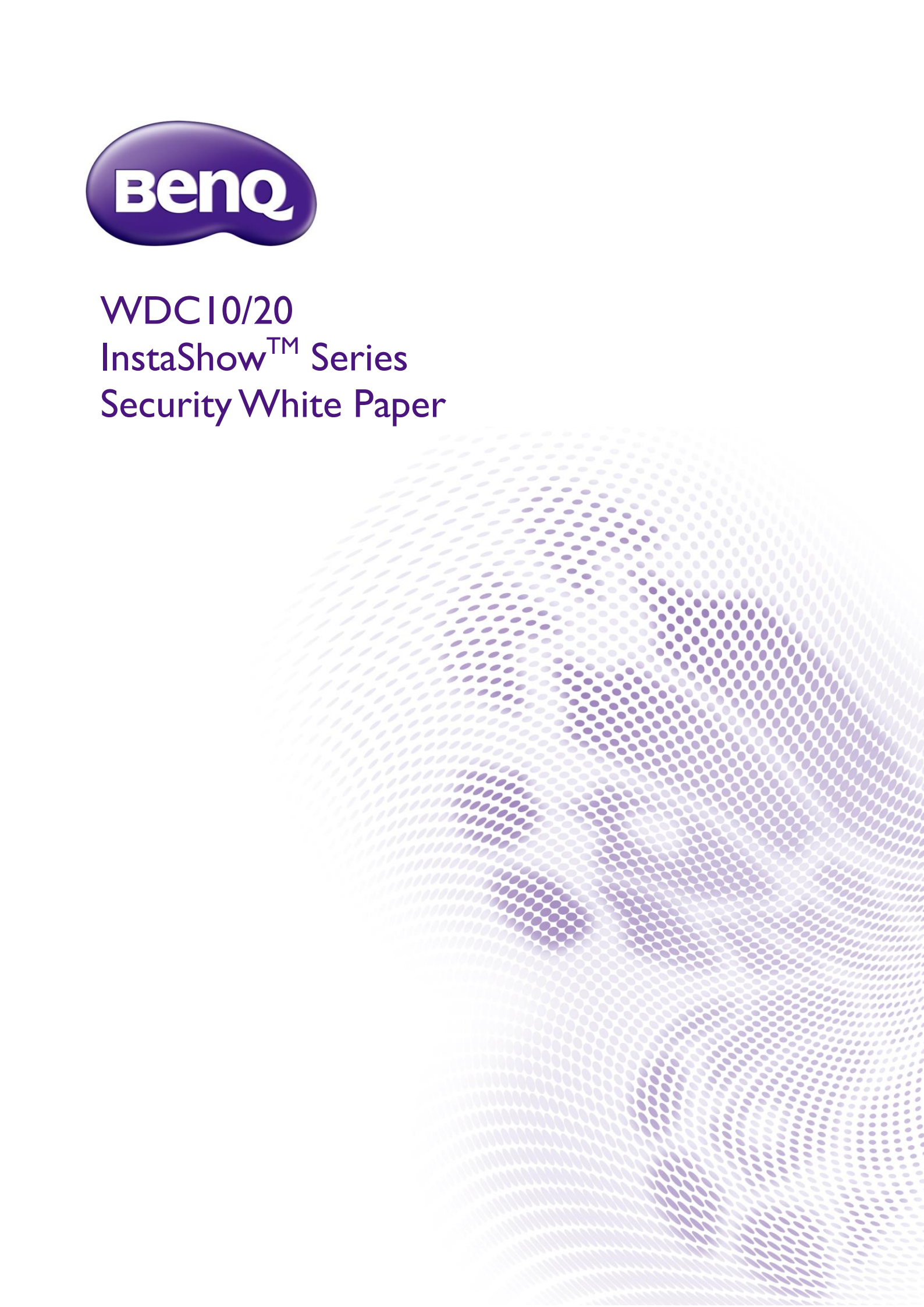


Table of Contents

Introduction

The InstaShow™ Series is a new-generation solution for business wireless A/V streaming display. This series of products includes WDC10, WDC10C and WDC20. Not only does it support the FHD resolution, it also supports plug and play, convenience of not needing to install drivers. Moreover it provides flexible network security options for IT personnel from various industries to configure appropriate network security settings. BenQ's new-generation solution for business wireless A/V streaming is to provide users with a good and secure wireless A/V streaming experience. In addition to basic wireless network packet encryption/decryption features, it moreover adds a unique network security handling mechanism to streamed packets that strengthens security of enterprise network environments and reduces burden of system maintenance on IT personnel. As the InstaShow™ Series supports two types of video input interfaces, HDMI and USB Type-C. USB Type-C supports the DisplayPort video format through DisplayPort alternate mode and DisplayPort is called DP for short. If the A/V device on the user's end uses an HDMI or USB Type-C interface and the USB Type-C supports DP alternate mode, then you can connect the transmission device of InstaShow to the A/V source device. Plug and play does not require you to install additional software and the benefit is it can get rid of malicious software attacks or threats from backdoor programs to reduce concerns about products from users.

The InstaShow™ Series System

In 2014 BenQ released the first-generation wireless A/V transmission product, WDP02 and launched the first-generation business wireless streaming display solution, InstaShow™ (WDC10), in the following year. After that BenQ released the second-generation business wireless streaming display solution, InstaShow™ S (WDC20). Through releasing InstaShow™ series of products BenQ delivered the concept of intuitive, stable, and secure wireless A/V streaming to the business display market in order to provide enterprise users with more comprehensive and thoughtful choices.

InstaShow™ Series Setup

The main device of InstaShow™ WDC10/WDC10C comes with one receiving device (Host) and two transmission devices (Button). The user just needs to connect one Button to the A/V source device and then click the button on Button, then the display device connected to Host will instantly display the video screen of the A/V source device. The other Button can also be connected to another A/V source device, the user only needs to click the button on this Button and then the screen on the display device will be switched to the video content of the A/V source device connected to this Button. None of the above operations needs installation of any software.

The InstaShow™ S — WDC20 is an advanced version of WDC10/WDC10C. In addition to performing the wireless projection function through a Button, a BYOD (Bring Your Own Device) wireless projection application is also added to give the user the ability to use iOS or Android devices directly without using a Button to wirelessly project to the display device connected to the Host. The Host is not only a receiving device of the InstaShow™ Series, but also the core of the entire system. The Host is mainly responsible for receiving the streaming data transmitted from a Button and ensures A/V can be stable and correctly projected to the display device. The Host of InstaShow™ can be connected to 16 Buttons wirelessly simultaneously, and the Host of InstaShow™ S can connected to 32 Buttons simultaneously. The IT personnel in an enterprise can add the Host to the enterprise network through the LAN port on the Host. When the Host becomes one of the devices in the enterprise network, IT personnel can then connect to the Web UI of the Host through the network to manage the device status of the InstaShow™ Series remotely. Even if the Host becomes an enterprise LAN device, external threats still could not acquire the A/V streaming data between the Host and a Button through intrusion by phishing or penetration.

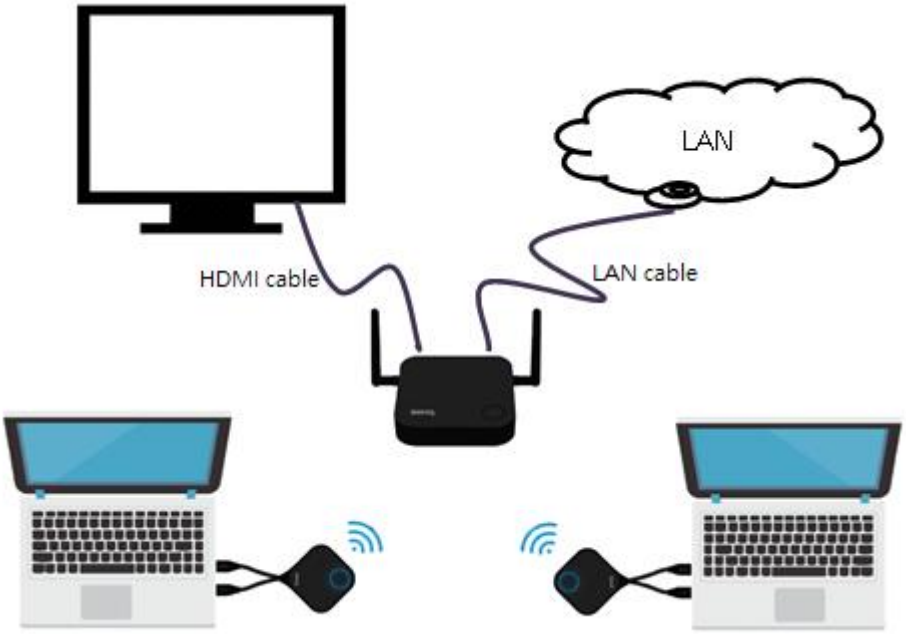
A Button is the transmission device in the InstaShow™ system. We support two types of interfaces for the Button, HDMI and USB Type-C in which USB Type-C supports the DisplayPort image format through DisplayPort alternate mode. There are two buttons on the HDMI Button, one is an HDMI cable and the other is a USB Type A cable.

The USB Type A cable is responsible for providing power to the Button and the HDMI cable is responsible for HDMI-formatted A/V data. HDMI devices have become quite popular and common on the market. For example most laptops, PS4, Blu-ray DVD players come equipped with HDMI ports.

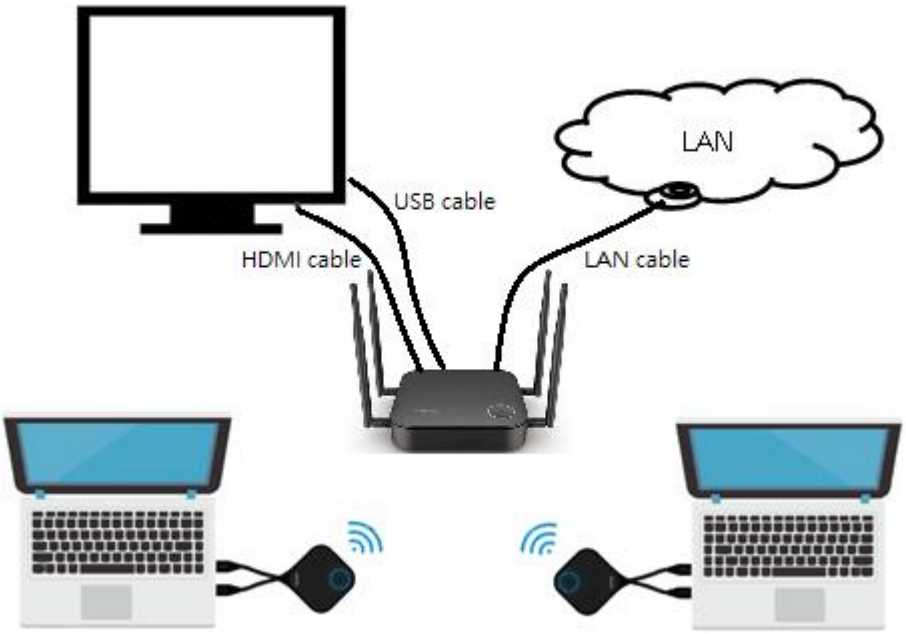
The USB Type-C Button only provides power to the system trough a single USB Type-C cable (supports DisplayPort alternate mode) and at the same time receives DisplayPort-formatted A/V data. Commonly seen USB Type-C devices include laptops. mobile devices and so on. Since some USB Type-C devices only support data transmissions by common file formats and does not support DisplayPort alternate mode. That means it cannot transmit the A/V formatted signals. Therefore before using the USB Type-C Button, the user has to make sure the USB Type-C port on the A/V source device supports DisplayPort alternate mode.

Based on the functions of the first generation InstaShow™, InstaShow™ S can moreover connect to HID devices (such as touchscreens, mice) through the USB Type A port on the Host to transmit control signals on the HID device to the Button through the USB cable. Therefor the USB cable on the Button in the InstaShow™ S not only provides power, but also supports receiving of HID commands to send back the HID commands received from the USB Type A port on the host with encryption wirelessly to the Button. After that the Button can send back the HID commands to the A/V source device through the USB Type A port connected to the A/V source device.

Single click the Button, and the Button will encode and compress the DisplayPort A/V signals sent from HDMI or USB Type-C and then transmit to the display device connected to the Host through the wireless network.



InstaShow™ Setup



InstaShow™ S Setup

System physical interface and firmware introduction

The InstaShow™ Series uses an embedded Linux and/or AOSP (Android Open Source Project), responsible separately for

. Bootloader access

.Linux CLI access

.Android Runtime access

Physical I/O on the Host:

.LED

GPIO control

.Button(s)

GPIO Scan

.RJ-45(Ethernet):

Web UI

REST API

Communication with Client

.Wi-Fi:

Web UI

Communication with Client

. USB Micro-B(InstaShow™)/ DC Jack(InstaShow™ S)

Power supply

.USB Type A(InstaShow™ S only)

Connect to HID device

.HDMI

Video / Audio output

Physical I/O on the Button:

.LED

GPIO control

.Button(s)

GPIO Scan

.Wi-Fi:

Communication with Host

.USB Type A:

Power supply

.HDMI:

Video / Audio input

.USB Type-C(Supports DisplayPort video format):

Power supply,Video / Audio input

The InstaShow™ Series is a strong security system

To solve the threats of wireless networks and enhance network security, BenQ gets rid of network threats through system modularization and thus has designed a wireless A/V streaming conference presentation system without the need to install software, the InstaShow™ Series.

The power consumption module system

The Button's power system in the InstaShow™ Series uses DC 5.0V converted to DC 3.3V as the main power voltage for the Button. According to the law of conservation of energy, electric current can be raised through lowering the voltage, allowing small power to support operations of the Button. The power specs of the Host in InstaShow™ S is DC 5.0V converted to DC 3.3V, the power specs of the host in InstaShow™ S is DC 12.0V converted to DC 5.0V and 3.3V. The power consumption module system in the InstaShow™ Series has passed 20,000 hour MTBF power certification, and the Host complies with (EC) No. 107/2009, (EU) No. 801/2013 and (EU) 2016/2282 regulations separately, providing the user with a trustworthy, stable and safe electrical design.

The A/V module system

The interfaces of the A/V source in the InstaShow™ Series are HDMI and USB Type-C. USB Type-C transmits DisplayPort A/V signals through supporting DisplayPort alternate mode. Because HDMI and DisplayPort are fully digitalized A/V signals, they support uncompressed audio and video signals and both are protected by HDCP regulations. The Host and Button in the InstaShow™ Series both comply with HDMI 1.4b (DPCP 1.2) and HDCP 1.4b(DP 1.2) certification standards. As long as the A/V source and A/V output device (sink) support HDMI 1.4b (DP 1.2) / HDCP 1.4b(DPCP 1.2), the source and sink can both be compatible with the InstaShow™ Series. The certifications the InstaShow™ Series have are ATCTW-16031 (Host), and ATCTW-16032 (Button).

The A/V encoding/decoding module system

Since HDMI and DisplayPort transmits uncompressed audio and video signals and the data amount from the uncompressed 1080P@60Hz audio and video signals is very tremendous, if the tremendous amount of streaming data hasn't gone through compression and transmitted wirelessly, the streaming data will take up extremely large amount of the bandwidth. To solve the problem of not enough wireless bandwidth, the InstaShow™ Series introduces unique A/V encoding and decoding methods to compress the bandwidth used by the tremendous A/V signals down to 40Mbps (InstaShow™)/20Mbps (InstaShow™ S) to provide the user with stable, smooth wireless A/V playing experience. Furthermore, in order to dedicate to balanced distribution of A/V quality and bandwidth used by the transmission, BenQ moreover introduces a dynamic encoding technology. Through this technology the compression ratio of A/V data can be adjusted dynamically to cope with the wireless bandwidth in the environment and make adjustments all the time.

The wireless transmission module system

The Wi-Fi transmission protocol used in the InstaShow™ Series is 802.11ac is coupled with WPA2 AES-128 bit encryption mode, WPA2 is the best encryption technology in the Wi-Fi 802.11ac standard.
If an InstaShow™ Series Host is used is the wireless station, then the Button is the client side equipment. Even though the Button belongs to client side equipment, the Button uses a closed system design. Therefore external threats cannot go through HDMI, USB Type A, or USB Type-C channels to threaten, penetrate and attack the system. The wireless transmission in the InstaShow™ Series has also acquired RF safety certifications like CE (EN 301 893), FCC (47 CFR FCC Part 15.407), NCC (NCC LP0002), and TELEC (ARIB STD-T71) of various countries.

The WAN/LAN module system

The InstaShow™ Series not only is a wireless A/V streaming conference presentation system, it also can be used as closed business wireless area network equipment. The WAN/LAN modules used in the InstaShow™ Series mainly provide users with network connection to the Host, and perform system configuration through the Web UI on the Host. Once the firewall is enabled through WAN on the Host Web UI, then external hackers cannot intrude into wireless communications equipment on the client side connected to the Host through WAN. You can also enable the channel isolation function through LAN on the Host Web UI to make network channels isolated in the clients connected to the Host to block communications between clients in the same network segment.

The Web UI management module system

The InstaShow™ Series provides users with a Host Web UI. Through the Web UI system status can be queried, Wi-Fi settings and system updates can be made. The user's connection device only needs to connect to the SSID network device name of the Host through Wi-Fi or uses the physical LAN to connect to the Host, then enters a valid account and password to log into the Host webpage, then the Web UI can be used immediately.

The light module system

The InstaShow™ Series provides LED lights to indicate equipment status. There is a three-color annular LED around the Button button, users can make sure of the current system status directly from the LED color and its on/off status. The LED brightness also depends on the light source usage scenario in most conference rooms and the design is to have soft and gentle brightness most suitable to the meeting presenter, not irritating to the human eyesight and providing users with more comprehensive conference experiences by covering even the smallest details.

The EMI/ESD module system

The network security design of the InstaShow™ Series can prevent hackers from attacking, and also follows product safety laws and regulations, compliant with EN55032 and EN55024 regulations.

The PCB module system

BenQ shoulders the social responsibility of reducing hazardous materials and environmental pollution. The PCBs used in the InstaShow™ Series all comply with lead-free, halogen-free green manufacturing fully. From control of raw materials, to manufacturing process, to quality control, inspection, and inventory taking before leaving the factory, they all have complete carbon footprint tracking and control mechanisms to fulfill the social responsibility as a citizen of the Earth and provide every part of the InstaShow™ Series a clean and friendly workspace.

BenQ ecoFACTS self declaration

Since 2001 all BenQ products have the ecoFACT label added to clearly tell you that BenQ products use green design and green materials.

Developing Earth friendly green products. BenQ will not only passively act to comply with requirements of green laws and regulations for our products, instead we actively work to make all products conform to green living and live again.

The InstaShow™ Series follows ecoFACTS regulations, meaning we declare we have done our best in aspects like getting rid of hazardous materials, choice of materials, packaging design, energy saving and so on.

Streaming flow protection

Through the system's modularized threat analyses, system network security can be classified into external hacker intrusion and internal protection management. Not matter what kind of threat it is, the purpose is none other than breaking and stealing.

Since the InstaShow™ Series does A/V streaming through a wireless network to achieve the goal of wireless presentation, the network system in the InstaShow™ Series uses firewall and channel isolation functions to prevent external hackers from intrusion. The A/V transmission formats are based on HDMI and DispalyPort without the need to install software to help realize wireless A/V streaming. You need to know that for enterprise users the biggest security threat is installing software. The InstaShow™ Series satisfies the needs of enterprise users of not needing to install software and also realizes the screen sharing function of multi-party conferencing to enhance the efficiency of enterprise conference presentations.

InstaShow™ Series system architecture

The operating procedure of the InstaShow™ Series is that the Button receives A/V streaming signals from the source (such as a laptop), and transmits A/V streaming signals to the Host through wireless means. Then the Host transmits the A/V streaming signals to the sink (such as a large screen or a projector) through the physical HDMI channel.

The processing procedure of the InstaShow™ Series system architecture is as follows:

(1) HDMI/DisplayPort signal decode

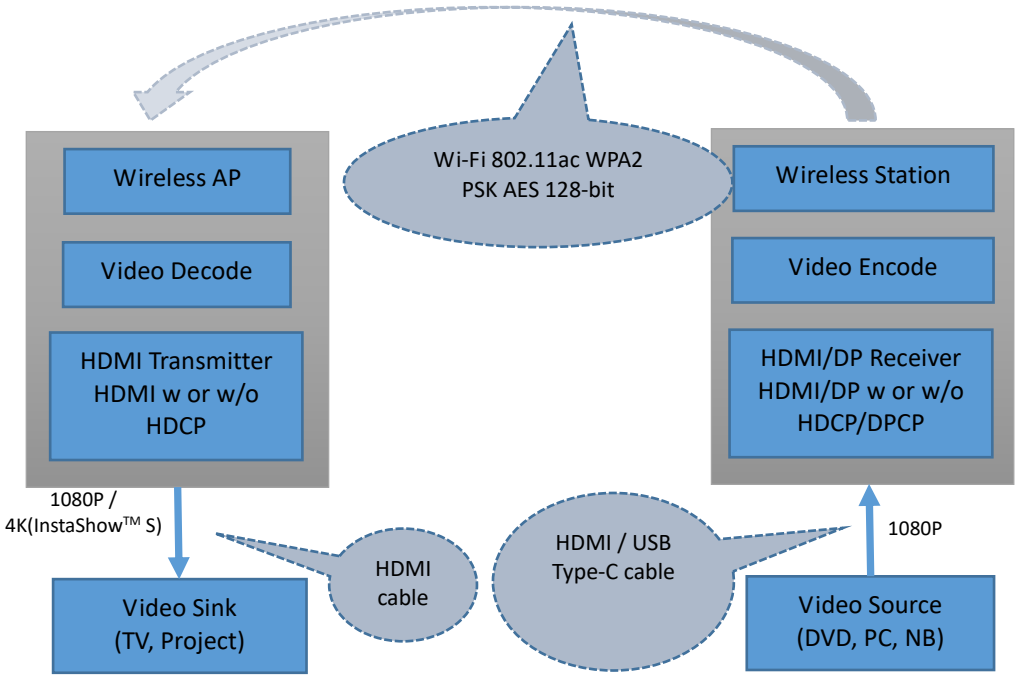
(2) Video and audio signal compress

(3) Video and audio stream with encryption over Wi-Fi

(4) Video and audio signal decompress

(5) HDMI signal encode

(6) HDMI output w or w/o HDCP



Flow	Transmission medium/interface		Note
HDMI/DP source	HDMI/DP Connect	Laptop, PS4 or BD/DVD player	
↓	HDMI/USBC cable	HDCP 1.4b or DPCP 1.2 or not(by content)	
Button	HDMI/DP Connect	1. HDCP or DPCP decode or not 2. Video and audio encode 3. Double encryption encodes	InstaShow™ Series
↓	Wi-Fi	***802.11ac WPA2 PSK AES 128-bit***	
Host	HDMI Connect	1. Double encryption decodes 2. Video and audio decode 3. HDCP encode	
↓	HDMI cable	HDCP 1.4b or not(depends on video content)	
HDMI sink	HDMI Connect	Display	

The InstaShow™ S Host is compatible with AirPlay and Google cast wireless projection technology to facilitate BYOD applications. Simply through iOS, Android devices the user can realize screen mirroring without holding the mobile device. In addition to this, the InstaShow™ S Host can also install the InstaShare app through iOS, Android devices. Using the InstaShare app to do wireless projection functions can also make the video transmission system of the wireless projection stabler and smoother.

The processing procedure of the InstaShow™ S BYOD system architecture is as follows:

(1) Video and audio captured

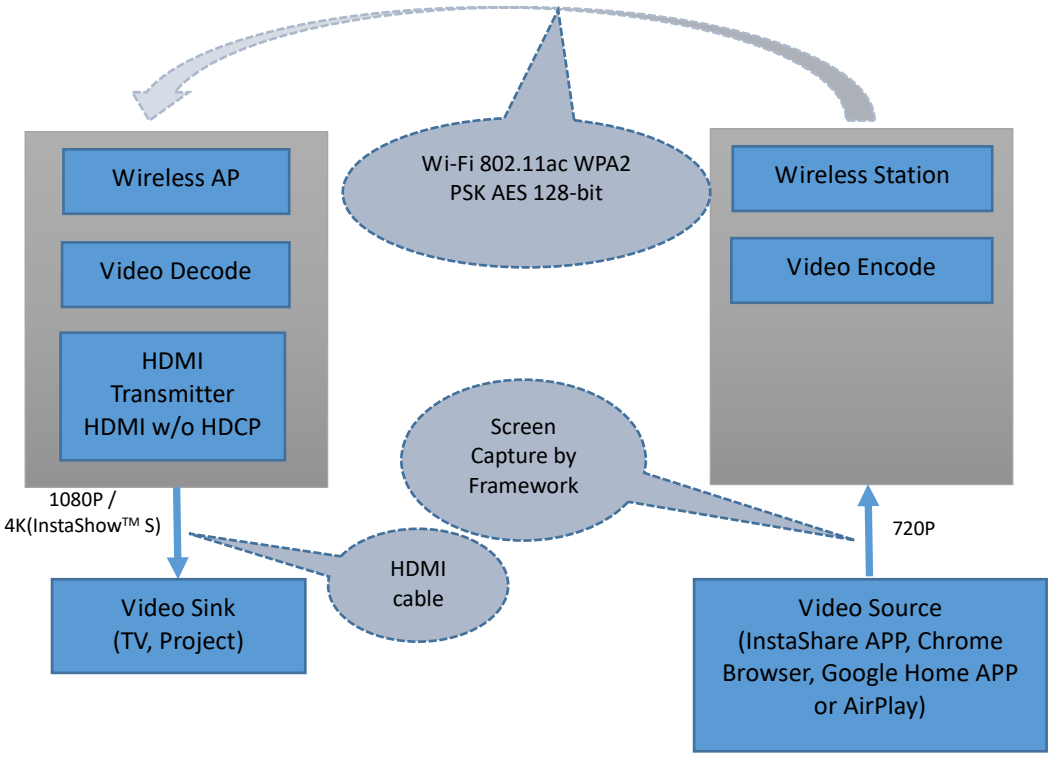
(2) Video and audio signal compress

(3) Video and audio stream with encryption over Wi-Fi

(4) Video and audio signal decompress

(5) HDMI signal encode

(6) HDMI output w/o HDCP

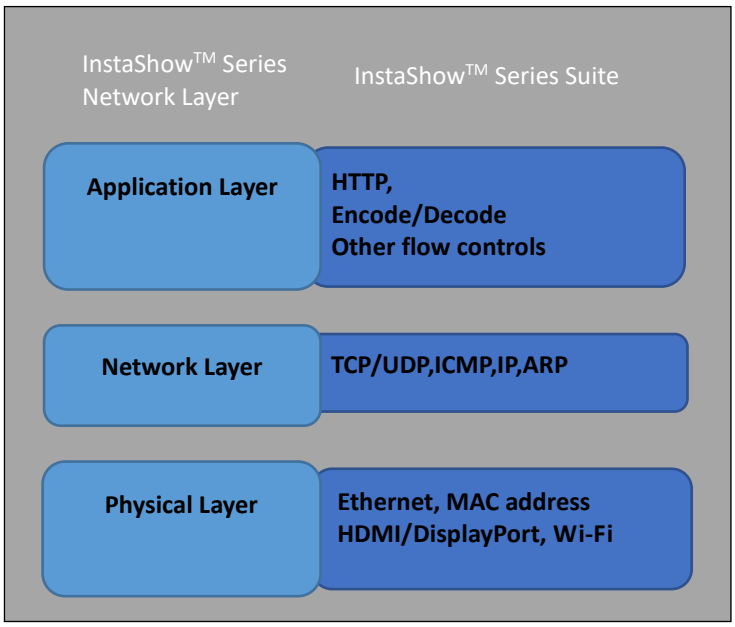


Flow	Transmission medium/interface		Note
BYOD	HDMI/DP Connect	1. Video and audio encode 2. Double encryption encodes	InstaShow™ S
↓	Wi-Fi	***802.11ac WPA2 PSK AES 128***	
Host	HDMI Connect	1. Double encryption decodes 2. Video and audio decode	
↓	HDMI cable	w/o HDCP	
HDMI sink	HDMI Connect	Display	

InstaShow™ Series network architecture

The InstaShow™ Series is a system with security, its system architecture completely matches data confidentiality, system completeness and functional availability. Network transmission methods are divided into physical networks and wireless networks. Physical networks have the advantage of absolutely free from interferences, wireless networks in general environments and spaces will be mostly subjected to electromagnetic interferences from neighboring frequency bands. As such the InstaShow™ Series has been treated to lower electromagnetic interferences to make electromagnetic waves not interfere with normal operations of wireless projections and is very suitable for enterprise conference and office applications.

The system architecture of the InstaShow™ Series has: physical layer, network layer, application layer. We will explain in detail each of the layers of the architecture.



1. Physical layer

The physical interfaces supported by the InstaShow™ Series include USB Type A/USB Micro-B, HDMI/USB Type-C (DisplayPort alternate mode) and RJ-45 (Ethernet) . Intruders might analyze the firmware program through the physical layer and load malware on the device. Therefore protecting the physical interface port of the device is equally important as protecting the other layers of the system.

USB Type A: Only provides the Button with DC 5V/0.9A power, does not support simplex/duplex data transmission functions.

> *The USB Type A of InstaShow™ S supports HID command transmissions, but does not support simplex/duplex data transmissions.*

USB Micro-B: Only provides Host with DC 5V/1.5A power, does not provide simplex/duplex data transmission functions.

HDMI: Responsible for input/output of A/V transmissions, supports HDCP protections.

USB Type-C: Supports DisplayPort alternate mode, responsible for input of DisplayPort format A/V data, the DPCP channel in its communication protocol supports the HDCP protection defined in the video.

RJ-45: Ethernet physical port. Provides users with login access to the Web UI of the Host to set up system functions, supports firmware updates but does not support Internet access functions.

The Ethernet of InstaShow™ S supports Internet w/ firewall function.

Since the authentication mechanism for communication connections between the Host and the Button will not go through the above-mentioned physical ports, hackers cannot get the data and parameters shared between the Host and the Button from these ports. But firmware update is an exception as the firmware update program needs to verify the completeness and signature of the firmware encoding format, otherwise it won't be able to support firmware upgrades.

As the InstaShow™ Series supports Wi-Fi network functions we treat Wi-Fi as a hidden port. The Wi-Fi port in the InstaShow™ Series has complete security controls in itself, the Host Wi-Fi provides verification when connections are made for the Host and the Button; when connection is confirmed, A/V transmission is then commenced. If other devices need to visit the application layer of the Host, then attached authentication is needed to ensure that control mechanisms like data confidentiality and system completeness are not broken.

2. Network layer

The network system in the InstaShow™ Series is divided into: WAN (Wide Area Network) and LAN (Local Area Network).

The WAN way is to connect to the network server through the RJ-45 port, the InstaShow™ Series enables the firewall to provide system network administrators the convenience to control the system fully in the application layer through the authentication mechanism of the enterprise network server(s). The network system and access control in the InstaShow™ Series is an independently working VLAN (Virtual Local Area Network) isolated from the enterprise network.

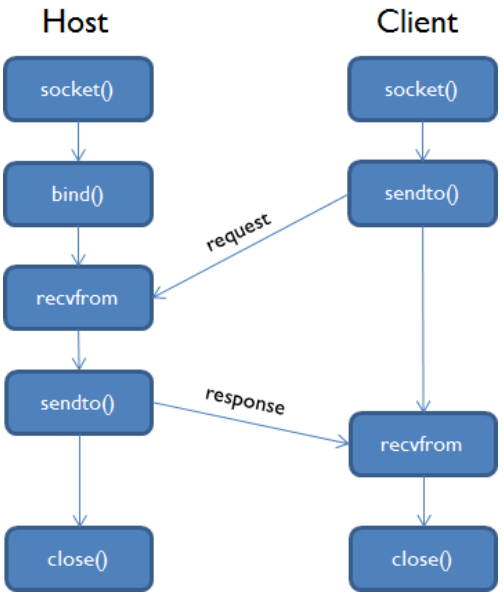
The LAN way is to establish LAN connections through Wi-Fi and the Button or other Wi-Fi devices. The protection mechanism of Wi-Fi is based on the security standard of 802.11i that provides WPA2-PSK to couple with a pre-shared key (PSK) as the authentication. WPA2-PSK encryption will ensure the confidentiality and completeness of all the data passing through wireless communications. The data encryption mode used is AES with 128 bits of key length, the limit on the key length has to be between 8 and 63 bits. Completeness is an examination method that goes through the Counter Mode CBC-MAC protocol (CCMP) and coupled with MIC (Message Integrity Check). The WPA2-PSK password and SSID name can both be set up using the network administrator privilege through the Host RJ-45 port.

3. Application layer

The core operating system of the InstaShow™ Series Host and Button is Linux and Android.In terms of the application layer, it provides system configuration, wireless pairing management, wireless projection network performance management, A/V format conversion and A/V format encoding/decoding functions. We will describe each of the functions in the following.

Wireless pairing management: Before the system can work fully, the Host and the Button need to establish a Wi-Fi connection first. Network connection is established in the TLS (Transport Layer Security) layer of the network layer, the Host end needs to ensure if the Button has passed the security authentication mechanism in the InstaShow™ Series upon creation of the identity authentication. After connection is established between the two parties, the Host still needs an additional Button verification step (MAC address).

Wireless projection network performance management: The transmitted content of the wireless projection is transmitted through UDP (user datagram protocol). This is because UDP doest not need to establish a handshake between the Host and the Button first, thus the connected communication efficiency is very high. In the UDP architecture figure, the client needs to initiate a request first, through two steps (socket and sendto) to do it, and the network server also needs to do three steps before it can receive messages from the client (socket, bind, recvfrom).



A/V format conversion and A/V format encoding/decoding: A/V streaming data conversion is an important link in the InstaShow™ Series. HDMI/DisplayPort A/V data at 1080P video resolution takes up about 6GB of space after lossless compression. Even though the InstaShow™ Series uses 802.11ac wireless network bandwidth and speed, the network bandwidth and data transmission speed are still not able to cope with 6GB of data. Therefore the InstaShow™ Series treats the A/V data with the four steps of format conversion, compression, decompression, and restoration through a high-performance core processor and then uses dynamic compression ratios to adjust the compression ratio. Moreover it is coupled with wireless projection network performance management to make high picture quality play stably and smoothly.

System configuration: The InstaShow™ Series system configuration uses a Web UI to ensure authenticated connections through HTTP service. HTTP is for non-business devices to use browsers to directly transmit data in clear text. Interactive conversations under an ordinary (insecure) mode will have hidden threats in the transmitted content as they are prone to theft by those with malicious intent. As such we make the user's login status bound to the Web login page of the Host. Within the valid time period the user's login status remains valid until the user account privilege has been revoked or cookie session has timed out.

Security class: The InstaShow™ Series has 3 security classes, differentiated based on the number of times the provided function has.

Class 1.

. The Button and the Host get needed identity authentication and password through a Wi-Fi connection.

. IOs, Android devices and the Host get needed identity authentication and password through a Wi-Fi connection.

. Account and password needed by the user to log into the Host Web UI.

Class 2.

. Make sure the MAC address of the Button is in the Host list for the Host and the Buton to establish connections.

. Firewall function enabled.

. After the InstaShare app is installed on a device, it can connect to the Host and needs to make sure the Host supports InstaShare before a connection can be established with the Host from that device. (InstaShow™ S only)

. The Host Web UI provides settings of enabling and disabling for BYOD applications. (InstaShow™ S only)

. Screen Lock on Web UI setting. (InstaShow™ only)

Class 3.

. Connection through the InstaShare app to the Host needs the paired PIN code to be entered. (InstaShow™ S only)

. No access to Web UI via Wi-Fi (InstaShow™ only)

Conclusion

The design concepts of the InstaShow™ Series are: ll pure H/W solution, plug & play, no need to execute or install software, intuitive operation without additional learning. The InstaShow™ Series can provide comprehensive protection of transmitted data, BenQ will keep on protecting the environment and delivering a friendly product use experience. BenQ promises not to implement or hide system backdoor programs and collect other data, you can use our products with ease and enjoy intuitive, secure wireless projections, and effectively make conference pesentations.