Barco

Wi-Fi and Security Considerations for ClickShare

Authors

David Martens, CISSP
David.Martens@barco.com

Guy Coen
Guy.Coen@barco.com

WI-FI CONSIDERATIONS

The right choice of frequencies and channels in larger-scale Wi-Fi deployments requires detailed knowledge of radio frequency (RF) and Wi-Fi technology and appropriate tools such as spectrum analyzers. A thorough treatment of this subject is beyond the scope of this white paper. Here, we will limit ourselves to providing some hints and tips to assist you with smaller-scale and non-critical installations. In all other cases, we strongly recommend that ClickShare be installed by professional integrators with a thorough understanding of RF and Wi-Fi technology.

- The 2.4-GHz frequency band is usually very crowded. Since ClickShare also has 5-GHz capability, we recommend using this frequency band instead.
- To select an appropriate channel within the chosen frequency band (among the channels allowed by the country concerned), we recommend using a Wi-Fi channel visualization tool such as the freely available InSSIDer tool from MetaGeek, which is available for the Windows and Mac OS X platforms. This tool will show you which channels are already occupied and which are not. Choose a channel that is still free, or that contains only weak signals from other access points (APs).
- ClickShare follows individual country regulations for the channels offered in each frequency band. Every ClickShare Base Unit is factory set for a specific geographic region. The administration interface will offer only the channels legally allowed by that setting. The factory-set region code cannot be changed once the Base Unit has left the factory, nor may a ClickShare Base Unit be installed outside the region for which it was intended. This intended region is indicated in the article number at the bottom of the Base Unit.No such restrictions apply to the ClickShare Buttons.
- ClickShare does not automatically hop to other channels based on changes in the RF environment. We therefore advise regular checks in environments where frequent changes occur in Wi-Fi and other RF equipment.
- In most cases, your company's IT department will have a clear overview of the frequencies in use for different applications in different areas of the company. We highly recommend that you involve the IT department in your Wi-Fi deployment.

IEEE 802.11n

ClickShare allows the use of IEEE 802.11n, which has significant advantages compared to legacy wireless technologies. For example, it offers improved performance, coverage, and robustness compared to older IEEE 802.11 standards (IEEE 802.11a/b/g), and it can use both the 2.4-GHz and the (less crowded) 5-GHz bands. It remains a wireless technology, however, which means that successful deployment requires careful planning based on sufficient knowledge of the technology.

The key advantages of IEEE 802.11n include the following:

- **Frame aggregation.** 802.11n boosts media access control (MAC) layer performance by allowing 802.11n devices to aggregate several packets into a single packet, which avoids wasted overhead between frames.
- **Multiple input, multiple output (MIMO).** This technology uses multiple antennas at both the transmitter and the receiver. MIMO exploits the fact that RF signals reflect off objects in their paths, causing multipath interference. MIMO uses spatial multiplexing (the transmission of separate data streams at the same frequency over channels in different physical locations), thereby turning multipath into an advantage by making the channel more spectrally efficient.
- **Channel bonding.** In contrast to 802.11a and 802.11g, 802.11n can bond two 20-MHz channels together to form a single 40-MHz channel, which significantly boosts maximum throughput.

Some legacy hardware sensors used in enterprise wireless intrusion detection systems (IDS) may not be able to detect 802.11n APs. The same applies to network management tools, so make sure the spectrum analyzers you use support MIMO spatial streams and other 802.11n features.

ClickShare's real-world performance depends on many factors, including environmental interference, system design, radio configuration, network design, and building construction. We have designed ClickShare using best practices, but the environment always plays an important role. Factors that limit the performance of an IEEE 802.11n system include the following:

- **Legacy station support.** 802.11n access points can be configured to interoperate with legacy IEEE 802.11b/g/a devices. This will reduce performance, however, because those legacy systems typically consume more "air time," so that the faster 802.11n endpoints must wait for the slower legacy systems before they can use the WLAN.
- **No multipath reflections**. 802.11n uses multipath reflections to its advantage; therefore, environments with few or no multipath reflections reduce 802.11n's performance.
- **No channel bonding.** In the 5-GHz band, IEEE 802.11n can be configured to use bonded, non-overlapping 20-MHz channels. Without channel bonding, the IEEE 802.11n infrastructure is used below its full potential.

The following table compares the different IEEE 802.11 standards:

	802.11b	802.11g	802.11a	802.11n
Maximum signaling rate	11 Mbps	54 Mbps	54 Mbps	300 Mbps
Operating frequency band	2.4 GHz	2.4 GHz	5 GHz	2.4 & 5 GHz
Typical outdoor range	100 m	100 m	100 m	150 m
Typical indoor range	30m	30m	30m	50m
Non-overlapping channels	3	3	23	3 (2.4 GHz) 23 (5 GHz)
Interference sources	Bluetooth, microwave, ovens, baby monitors, etc.	Bluetooth, microwave, ovens, baby monitors, etc.	Cordless phones	Same as IEEE 802.11b/g at 2.4 GHz Same as IEEE 802.11a at 5 GHz

Operational modes

IEEE 802.11n access points can be used in multiple operational modes, each with advantages and disadvantages.

- **Mixed mode** enables 802.11n devices to coexist and interoperate with legacy 802.11b/g/a devices on the same WLAN.
- **Legacy mode** makes the 802.11n AP behave like an 802.11g/a AP. There will be some performance improvements due to a number of physical layer enhancements, but the performance remains below full potential.
- **IEEE 802.11n mode** provides maximum performance because the AP is not slowed down by legacy devices that consume greater "air time".

Channel selection per region

As stated above, the channels available vary between geographic regions. ClickShare obeys national regulations and offers only those channels allowed in the region listed on the product label (see the last two letters in the article number on the bottom of the Base Unit: NA for US and Canada, EU for Europe, CN for China, JP for Japan, WW for world-wide).

This is not the complete picture, however, because neighboring channels can potentially interfere. The 802.11 standard divides the 2.4-GHz range into thirteen 22-MHz-wide channels, spaced 5 MHz apart. These channels usually overlap, resulting in signal degradation. There are only three non-overlapping channels available in the IEEE 802.11 standard: channel 1 with center frequency 2.412 GHz, channel 6 with center frequency 2.437 GHz, and channel 11 with center frequency 2.482 GHz, as shown in figure 2. Clearly, access points located near each other should avoid overlapping frequencies.

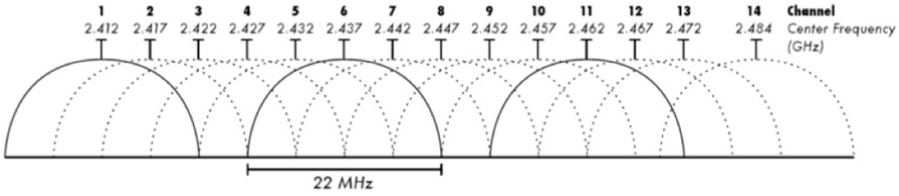


Figure 2: The 802.11 channels in the 2.4-GHz range

As previously stated, a detailed description of the technology is beyond the scope of this white paper. Here, we will provide a simplified view to illustrate the principle. For more complete information, please refer to the appropriate IEEE standards and local regulations.

ClickShare channels in the 2.4-GHz frequency band

Channel	Frequency (MHz)	NA	JP	EU	CN	WW
1	2412					
2	2417					
3	2422					
4	2427					
5	2432					
6	2437					
7	2442					
8	2447					
9	2452					
10	2457					
11	2462					
12	2467					
13	2472					

In 802.11g and newer standards, only channels 1, 5, 9, and 13 may be used, in order to obey the non-overlapping 20-MHz OFDM channel scheme borrowed from 802.11a. But please survey your site first; if channel 6 is heavily occupied, follow the three-channel system instead.

Note that channels 12 and 13 are available in the US under low-power conditions. Since ClickShare's built-in AP does not support power adjustment, however, these two channels are blocked for US-designated Base Units.

ClickShare channels in the 5-GHz frequency band
The picture for the 5-GHz frequency band is more complex than for the 2.4-GHz band.

The United States requires that devices operating on 5.250-5.350 GHz and 5.470-5.725 GHz must employ dynamic frequency selection (DFS) and transmit power control (TPC) capabilities. This is to avoid interference with weather radar and military applications. In 2010, the FCC further clarified the use of channels in the 5.470-5.725 GHz band to avoid interference with Terminal Doppler Weather Radar (TDWR) systems. This statement eliminated the use of channels 120, 124, and 128. Channels 116 and 132 may be used, as long as they are separated by more than 30 MHz (center-to-center) from a TDWR system located within 35 km (21.7 mi) of the device.

Germany also requires DFS and TPC capabilities on 5.250-5.350 GHz and 5.470-5.725 GHz. In addition, the 5.150-5.250 GHz frequency range is allowed for indoor use only. As this is the German implementation of EU Directive 2005/513/EC, similar regulations should be expected throughout the European Union.

Austria has adopted EU Directive 2005/513/EC directly into national law.

South Africa has adopted the European regulations.

Japan allows old APs supported by J52 to connect using channels 34, 38, 42, and 46.

The following table gives an overview (valid at the time of writing) of the channels that are supported in at least one of ClickShare's target regions:

Channel	Frequency (MHz)	NA	JP	EU	CN	WW
184	4920					
188	4940					
192	4960					
196	4980					
36	5180					
40	5200					
44	5220					
48	5240					
149	5745					
153	5765					
157	5785					
161	5805					
165	5825					

Important note: Channel availability is also related to signal strength, which is related to the antennas being used (among other things). If the user or integrator wishes to extend the Wi-Fi range by using larger antennas on the ClickShare Base Unit, Barco cannot guarantee that the new configuration will still meet locally applicable regulations.

Dynamic frequency selection

The ClickShare AP does not support DFS as specified in the IEEE 802.11h standard.

The 802.11h standard, commonly referred to as Dynamic Frequency Selection (DFS), was created to define a set of procedures to detect and avoid interference with radar systems operating in the 5-GHz range (UNII channels: 52–64 and 100–140). The part of the specification that is most visible to users is the ability of a DFS-capable AP to detect and move away from a channel that interferes with radar systems. APs that do not support DFS are not allowed to operate on the channels where interference occurs, which limits the number of channels available in the 5-GHz spectrum.

Signal propagation in the real world

Various mechanisms affect the propagation of radio signals. These mechanisms can be attributed to five major physical phenomena: **reflection, diffraction, refraction, scattering, and absorption** (Hucaby, 2007; Durgin et al., 1998; Sarkar et al., 2003). These basic phenomena distort the propagating signal, making it stronger or weaker. They can also create additional propagation paths beyond the direct line-of-sight path between the radio transmitter and receiver, resulting in multiple signals arriving at the receiver with different delays. This leads to shadowing and multipath fading, which affect performance.

In general, these phenomena depend on the surrounding environment and the frequency of the signal being used. Determining the effect of each of these phenomena for a given environment and frequency is a difficult task that gives rise to very complex models. Because IEEE 802.n uses MIMO, which involves multiple frequencies, the situation becomes even more complex.

Over the years, many mathematical radio propagation models have been developed to accurately predict the potential propagation of signals within an environment (Durgin et al., 1998; Iskander and Yun, 2002; Mikas et al., 2003; Garg, 2007). There are two basic approaches to modeling radio networks: the empirical or statistical method, and the deterministic method.

- The **empirical** method is based on site surveying and uses data gathered from the actual environment to be modeled.
- The **deterministic** method (also known as the ray-optical or ray-tracing method) uses software based on the theory of electromagnetic wave propagation.

Compared to the empirical site survey method, the deterministic method is usually more convenient and cost effective. By simulating different configurations of the environment where the network will be deployed, the method can reach an optimal configuration. However, the method depends on the availability of data such as the composition of the obstacles along the signal path and their corresponding effects on electromagnetic signals to generate an accurate prediction (Sarkar et al., 2003; Iskander and Yun, 2002; Mikas et al., 2003). In the absence of such data, site surveying is usually quicker and more accurate.

Power over Ethernet

The IEEE 802.3af standard for power over Ethernet (PoE) was developed to facilitate the deployment of WLAN APs in environments where power access is difficult. ClickShare is more than just a WLAN AP, however, because it also drives the projector or display and performs video processing on the incoming video streams. Therefore, the ClickShare Base Unit does not include PoE capability.

SSID broadcasting

To facilitate installation, SSID broadcasting is factory enabled; the integrator can switch it off before first use if desired. Note that for mobile app users, SSID broadcasting will significantly increase the system's ease of use.

WLAN controller

A WLAN controller is a device that provides centralized management and control of a collection of lightweight APs. The ClickShare Base Unit is neither a WLAN controller nor a lightweight AP, and cannot be operated as such.

Large-scale deployments

In the current product, every ClickShare Base Unit is both a display controller and a Wi-Fi access point. As such, the deployment of a large number of ClickShare systems is no different from the deployment of a large number of Wi-Fi access points.

There is no hard limit on the number of ClickShare systems that may be deployed. The greater the number of Wi-Fi clients on a Wi-Fi network, and the greater the traffic those Wi-Fi clients generate, the lower the performance of all clients in the same "area" of the network, but there is no single hard limit beyond which the network breaks down.

This white paper provides several hints and tips, but it is not intended to be a thorough manual on large scale Wi-Fi deployments. This is a very specific area of expertise. We strongly advise you to use professional Wi-Fi integrators for the analysis, planning, and deployment of such large installations.

As noted above, in the current version of the product, every Base Unit is both a display controller and a Wi-Fi access point. We also plan to add a management layer. This will allow the integrator additional flexibility in large-scale installations:

- A number of ClickShare Base Units will be able to use an external Wi-Fi network independent of ClickShare. The ClickShare Buttons will then wirelessly connect to that external Wi-Fi network, while the ClickShare Base Units will use a wired connection (through their Ethernet ports).
- All ClickShare Base Units will be able to be monitored, configured, and updated from one central web application, which simplifies installation and integration in a corporate IT network.

From the end user's point of view, ClickShare's operation in the meeting room will not change. Installation will be a bit more complex for the integrator and might require a project engineering phase, in close cooperation with your company's IT department, before rollout. The described extension will be made available to existing ClickShare systems as a software upgrade.

Recommendation

ClickShare is a closed system and is not intended to interoperate with other, more general purpose, APs. We therefore strongly recommend you use IEEE 802.11n mode in the 5-GHz frequency range to decrease the risk of interference. Every ClickShare Base Unit will use WPA2 PSK (Pre-Shared Key) technology to guarantee the confidentiality and integrity of wireless traffic between Buttons and Base Units.

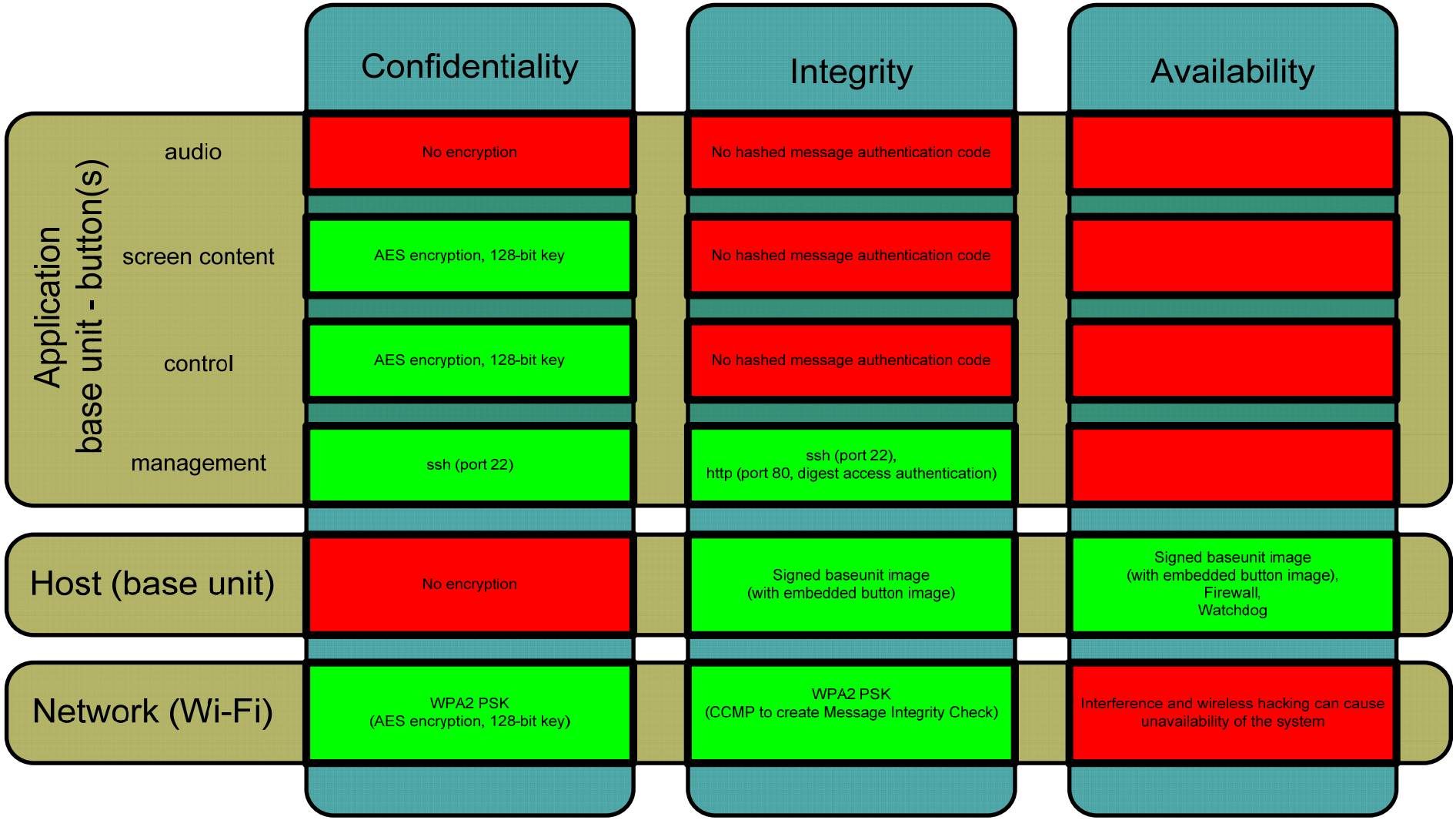
Security considerations

The cornerstone principle of information security is the CIA triad: confidentiality, integrity, and availability. All parts of a product or system must honor this concept throughout the system's life cycle to guarantee a secure environment.

Before addressing the security concerns you may have about ClickShare, we would like to emphasize one specific fact: the use of Wi-Fi communication makes the availability corner of the triad very fuzzy. Every source of interference in the vicinity of a wireless system can—intentionally or unintentionally—cause that system to function incorrectly and thus be unavailable. As stated above, we strongly advise you to use professional Wi-Fi integrators for the analysis, planning, and deployment of large installations; that way, you can at least eliminate unintentional interference. The proper functioning of your ClickShare system starts with an interference-free environment.

A communication system can be divided into three layers: network, host, and application. Mapping these three layers onto the CIA triad will reveal how security is implemented in your system and show you where safeguards are missing. By using a layered approach and applying multiple safeguards to protect an asset, you ensure that if one safeguard fails, the system will not be compromised.

Safeguards implemented in the ClickShare system (Base Unit and Buttons)



Malware on the client PC

The only application running on the client PC is the ClickShare client software. This piece of software is developed and maintained in-house by Barco, and no external party has access to it. The binary software image is signed before it is passed on to the factory that produces ClickShare, ensuring that no one has altered it and thus guaranteeing its integrity. The ClickShare code-signing certificate has been issued by GlobalSign, a WebTrust-certified certificate authority.

The software is stored on a mass storage device inside the ClickShare Button, which is read-only during normal use. It can only be programmed by the factory, or re-programmed by the ClickShare Base Unit. A normal user cannot write to this storage device, intentionally or unintentionally. All re-programming is done by software running on the Base Unit that is also developed, maintained in-house, and signed by Barco, with no access by any external party. Only signed images are permitted to upgrade the Base Unit, to guarantee the integrity of the software running on the Base Unit and to avoid tampering with the mass storage device inside the ClickShare Button.

The client software is never installed on any client PC (which would affect the PC's permanent storage and configuration); it merely runs on that PC (which only affects volatile RAM memory and the CPU). The software does not require any special drivers to be installed on the PC and does not install any drivers itself.

This makes it virtually impossible for malware to enter the client PC through the ClickShare Button.

Content captured by ClickShare

ClickShare captures only the visual information that is rendered locally on screen and the audio that is playing at the moment the content is shared. Barco guarantees that no other files or data are streamed or sent from the client PC to the ClickShare Base Unit.

In the Wi-Fi layer, WPA2-PSK encryption ensures the confidentiality and integrity of all data passing through the wireless channel. Confidentiality is provided by the AES block cipher with a 128-bit key length. Integrity is provided by using the Counter Mode CBC-MAC Protocol (CCMP) to create a Message Integrity Check (MIC). Using the WPA2-PSK passphrase and SSID, both of which can be configured by the administrator in the Base Unit web interface, a set of temporary keys is derived that are used for authentication (CCMP) and encryption (AES), in accordance with the IEEE 802.11i security standard.

In the application layer, the screen information is encrypted a second time using the same AES block cipher with 128-bit key length to guarantee end-to-end confidentiality. This 128-bit key is randomly generated per session and exchanged using the RSA-OAEP encryption scheme with a 1024-bit public/private key pair. In the near future, audio will be encrypted the same way to guarantee application-layer confidentiality for both screen content and audio data. In potential future scenarios where ClickShare Buttons wirelessly connect to an external Wi-Fi network and access the Base Unit over the wired interface, the ClickShare

solution can already guarantee end-to-end confidentiality. The Android and iOS apps do not yet provide this additional application layer security, but it will be implemented in the near future. (Of course, confidentiality and integrity are already guaranteed by the Wi-Fi layer if the mobile device is connected directly to the Base Unit's wireless interface).

Note also that the Base Unit acts as an endpoint for the information stream: information sent to the Base Unit is not distributed to any of the client devices.

All these safeguards make it virtually impossible to tap into the information stream and recover the original data.

Penetration testing the ClickShare system

ClickShare has several interface points that can be used to attempt system entry and attack:

- **Base Unit wired interface**: This interface is not currently used to share content; it is used only for remote administration. The Base Unit does not initiate any external connections over the wired interface. As an endpoint, it only opens a limited number of ports:
    - TCP port 22 (SSH): for access by certified level-3 service technicians only
    - TCP port 80 (HTTP): for administration via the web interface

- **Base Unit wireless interface**: This interface is not intended as a general purpose AP. It does not forward any packets and it is protected using WPA2-PSK encryption. The following ports are accessible through this interface:
    - TCP port 22 (SSH): for access by certified level-3 service technicians only
    - TCP port 80 (HTTP): for administration via the web interface
    - UDP port 514 (rsyslogd): to send Button logs to the Base Unit. The logs are sent unencrypted in the application layer, though they are encrypted in the Wi-Fi layer
    - TCP ports 1688, 1689, 3268, 8080, and 9870: for incoming connections from Barco mobile apps (Android and iOS)
    - TCP port 9876: for incoming connections from Buttons

- **Button**: The Button's wireless interface is limited by its firmware to connect only to the AP on the Base Unit, using the WPA2-PSK key exchanged during pairing. The following ports are accessible through this interface:
    - TCP port 22 (SSH): for access by certified level-3 service technicians only

- **Base Unit USB port**: We recommend you do not extend access to these USB ports through USB extenders beyond the physical boundaries of the meeting room. In normal use, the USB ports support only three devices:

- ClickShare Button: used to pair the Button with that particular Base Unit and to update the software residing on the Button. This process is handled entirely by server-side software running on the Base Unit.
- USB pen drive: used to upgrade the software on the Base Unit itself. This process is handled entirely by server-side software running on the Base Unit. The software checks the content on the USB pen drive by searching for a valid signed image for the Base Unit. This makes it impossible to change the Base Unit software using a USB pen drive containing malicious software.
- Keyboard: used only by certified level-2 service technicians in the event of problems. Access is protected by username and password credentials, making it impossible for unauthorized users to access the system via keyboard.

The wired and wireless Base Unit interfaces are separated from one another by a software firewall, and there is absolutely no traffic traveling between the two interfaces. No client accessing the wireless interface will have access to the network to which the Base Unit is connected via its wired Ethernet interface. The drawback to this approach is that mobile devices connecting through the app will not have Internet access through their Wi-Fi interface once they connect to the Base Unit.

SSID cloaking

Keep in mind that SSID cloaking can provide a false sense of security. Using tools freely available on the Web, it is fairly easy to scan an area for hidden networks; it is therefore extremely important to add 802.11i (WPA2) protection to any wireless solution to guarantee the confidentiality and integrity of traffic in the air. ClickShare is fully WPA2-capable.

Base Unit management

Base Unit administration occurs through the HTTP interface using a web browser. The administrator authenticates using username and password credentials via digest access authentication. The default administrator username and password are both *admin*; we strongly recommend you change the password the first time you log in. The Base Unit does not currently place specific requirements on passwords, so it is up to the administrator to choose a password that is secure and that cannot easily be guessed using a dictionary attack. Future implementations will provide an HTTPS interface and a password policy configurator, where minimum requirements can be set and accounts can be blocked for a certain period of time after a specified number of unsuccessful access attempts.

The Base Unit accepts incoming SSH connections. These connections are encrypted and access is authenticated using username and password credentials. Only certified level-3 service technicians may access the unit through SSH. SSH access can be disabled in the web interface.

Patch management

The Base Unit and Button run an embedded Linux OS with multiple open-source software packages. A list of these packages and their versions is available per release on request. Barco closely monitors new vulnerabilities detected in open-source packages embedded in our products. If we detect a serious vulnerability, we will provide you with a new signed Base Unit image that patches the vulnerability as quickly as possible.

Disturbing the meeting

It is possible to abuse the system by pairing a Button with the Base Unit in the meeting room before the meeting starts, or connecting and sharing with the mobile app, in order to show unwanted content from outside the meeting room (within Wi-Fi range). This is a known and accepted security risk in the system. It could potentially hamper the availability of the ClickShare system during a meeting, but the confidentiality and integrity of the data traffic between clients and the Base Unit are never compromised.

Every Button that shares content with the Base Unit does reveal its user on the central screen (the name of the user as read from the operating system configuration). Any user showing unwanted content must be in the vicinity of the Base Unit and can easily be traced. Such abuse can also easily be thwarted by resetting the WPA2 password in the administration interface at the beginning of a critical meeting, then pairing only the Buttons present in the meeting room and providing the password only to the mobile-app users participating in the meeting. This is why we strongly recommend you do not extend access to the Base Unit USB ports beyond the physical boundaries of the meeting room.

Logging

The ClickShare system contains an extensive logging engine based on rsyslog. No individual Button stores logs; rather, the Buttons forward all messages to the rsyslog server running on the Base Unit. The Base Unit also logs its own activities. The log files can be downloaded via the web interface by users with admin access. The data stored in the log files contains information about the current system state: component temperature, frame rate statistics, statistics on the wireless link quality, number of connected users, MAC addresses, and so on. If the "Debug logging" check-box is checked in the Base Unit web interface, the username of the person currently sharing will also be logged. In any event, no data from the screen or audio capture is reproduced in the log files.