



Wireless Collaboration in Enterprise Environments

Wireless presentation systems have flourished in the past decade due to advances in computing power and wireless technologies. The original goal of wireless presentation was to solve the problem of attaching external displays to the computing devices as simply as VGA and HDMI without the cost and inconvenience of fixed cable installation. As the ubiquity of mobile devices in enterprise environments increased, the pressure to install wireless display solutions correspondingly increased in priority.

The proliferation of touch-screen solutions and interactive whiteboarding in recent years has further altered the paradigm of pure-play wireless presentation into one of wireless collaboration. The explosion of alternative meeting spaces such as huddle rooms requires mass-deployable solutions with low total cost of ownership.

The intersection of enterprise security and effective management of wireless spectrum with wireless presentation and collaboration creates additional deployment challenges. The inherent security of one-way wired video connections to display systems is difficult to replicate in wireless presentation and collaboration due to a multitude of factors. When BYOD devices for guests or other users become a factor, the issues of security and wireless management becomes even more difficult to address effectively.

This white paper gives an overview of the requirements to manage all the above factors effectively within any enterprise environment. Most of these principles apply to enterprise-like deployments in government or higher education, and non-enterprise environments for small business or K-12 deployments.

Security and Wireless Framework

Security of proprietary information, devices and networks in enterprise environments is an ongoing process. Organizations typically develop certain baselines depending on the risk model for accidental information exposure and invasive threats such as viruses and network intrusion. These baselines often include limiting user-level installation of software and storage connectivity over USB or the network by the device administrator. Many organizations also deploy mobile device management solutions to lock down even approved app usage on devices, requiring special wrappers or libraries for the app to run securely. On a network level, sequestering guest traffic allows isolation of potential threats to and ensures quality of service for information infrastructure and devices. Further sequestering of network broadcast traffic may be necessary when Apple devices are used in an organization, as Apple wireless display requires the use of broadcast protocols such as Bonjour to announce their presence to devices when such broadcasts are not cacheable at Wi-Fi access points. In many cases, systems that allow guest access must be fully isolated without any connection to enterprise networks. Protection using rotating passwords or hidden passwords for end users is necessary to ensure only authorized presenters access the room display.

A specific concern to network infrastructure is wireless spectrum management. Wireless access points are the entry point of most organizations' user device connectivity, requiring careful management of limited wireless spectrum. The primary bands for Wi-Fi – 2.4GHz and 5GHz – are often congested from unmanaged devices, requiring organizations to manage Wi-Fi channels and power carefully to ensure quality of service. In some cases, organizations require consolidation of wireless traffic strictly to organization-managed wireless access points rather than other access points. In cases

A specific concern to network infrastructure is wireless spectrum management.

Wireless Collaboration in Enterprise Environments

where full isolation and native device support is required, Miracast in peer-to-peer (P2P) mode and infrastructure mode is a requirement for Windows devices, as is the ability to add an access point for organizations that do not restrict third-party access points to facilitate iOS/macOS screen mirroring on Apple devices. P2P Miracast must also include AGO mode functionality to avoid Wi-Fi access point conflicts by using pre-chosen channels rather than the NGO mode found in consumer grade devices where the wireless channel is dynamic.

Management and User Deployment Concerns

During and after commissioning of wireless presentation and other professional AV equipment within an enterprise, additional concerns arise regarding ongoing maintenance. Centralized management is a critical part of deployment of wireless collaboration systems to monitor units, reconfigure groups of units, and upgrade firmware for features and security. For organizations that desire touch capability on front of room screens, integration with standard USB HID touch displays and Microsoft Office 365 tools is preferable due to their pervasiveness. As virtually all new deployed room displays are 4K or UHD resolution, supporting these resolutions is also strongly desired for future proofing. A consistent, simple, easy-to-use natively-supported front of room experience for users of wireless collaboration is strongly preferred to minimize user confusion.

For user devices, organizations prefer solutions without apps for Windows, iOS, macOS and Android due to user training and management of user devices. Native extended desktop support is also essential for user privacy and duplicates wired display experiences. Collaboration using Office 365 tools is similarly essential for productivity and centralized storage of touch-input content. Fast and reliable user connections with fewer connection steps are critical, including for guest users on multiple platforms, to increase productivity and reduce time spent connecting.

Centralized management is a critical part of deployment of wireless collaboration systems to monitor units, reconfigure groups of units, and upgrade firmware for features and security.

Wireless Collaboration Constraints and Use Cases

Based on the above, the selection of a single wireless collaboration solution must consider the following constraints:

- App access or installation may be limited or disallowed
- Access to device USB may be limited or disallowed
- Native screen mirroring and extended desktop on any major OS must be supported
- Multiple isolated network connections to the solution must be supported
- Multiple wireless bands, channels and power must be managed and accommodated
- Simultaneous Miracast P2P AGO mode and Miracast infrastructure mode for Windows and Android devices with iOS/macOS screen mirroring for Apple devices must be supported
- Touch collaboration tools leveraging Office 365 must be supported
- 4K capability with standard USB HID touch for touch room displays must be supported

With security and wireless requirements in mind, three primary cases emerge for wireless presentation systems compatible with modern enterprise networks:

1. Full enterprise network isolation
2. Guest and enterprise network isolation
3. Guest and enterprise network isolation with Apple isolation

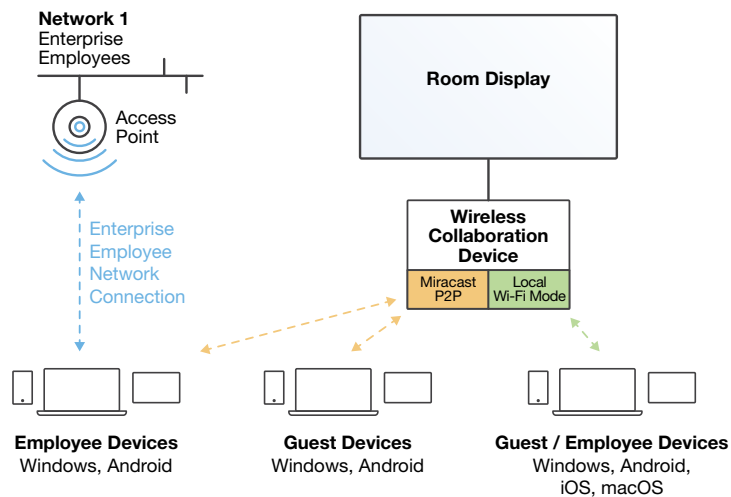
Enterprises choose full network isolation when security of the network relative to the room is paramount.

Full Enterprise Network Isolation

Enterprises choose full network isolation when security of the network relative to the room is paramount, particularly for guest devices, or when IT staff disallow network infrastructure access to proAV equipment.

To support this configuration, the device should provide:

- Miracast P2P for guest or employee users via P2P wireless
- iOS/macOS screen mirroring for guest or employee users via local Wi Fi
- Touch screen for Windows 10 Miracast P2P users via USB to the display
- Easy on-screen instructions for connecting via either protocol



All constraints for security, network, management and user deployment are met. No apps or USB dongles are used, no added training is required, and users of all major operating systems can be accommodated. Management of the device's bands, channels and power for Miracast P2P AGO and local Wi-Fi access point ensures optimal user experience and co-existence with existing nearby Wi-Fi access points. Touch screens are supported when available.

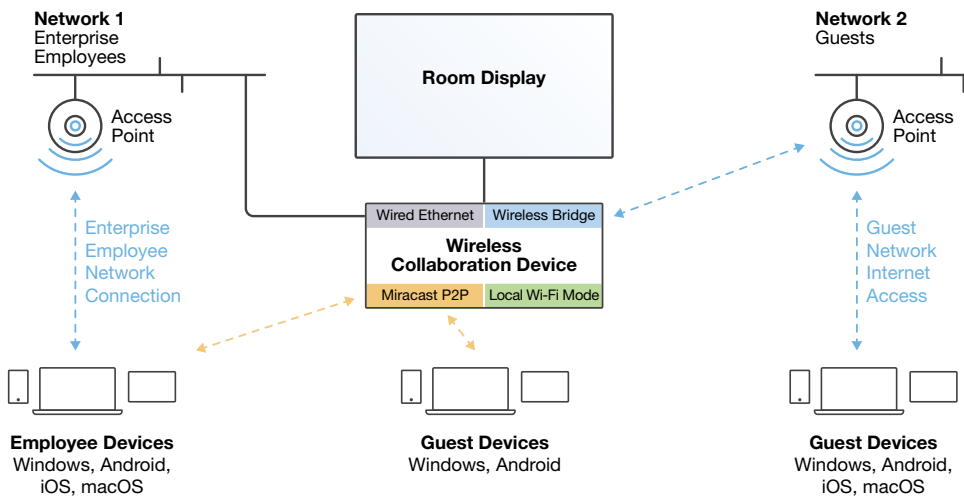
The disadvantage of this system is lack of network or Internet access for all users except Miracast P2P users with another connection such as mobile hotspot or Wi-Fi access point.

Guest and Enterprise Network Isolation

Enterprises connect wireless collaboration devices to guest and enterprise networks simultaneously when guest Internet connectivity is required for collaboration alongside employee access, when isolation can be maintained for employees to access enterprise network resources securely and when use of corporate network resources such as access points is mandatory.

To support this configuration, the device should provide:

- Miracast P2P for guest or employee users via P2P wireless
- Miracast Infrastructure and iOS/macOS screen mirroring for employees via enterprise employee network Wi-Fi access point through the device's first network interface
- Miracast Infrastructure and iOS/macOS screen mirroring for guests via enterprise guest network Wi-Fi access point through the device's second network interface
- Touch screen for Windows 10 Miracast users via USB to the display
- Easy on-screen instructions for connecting via either protocol



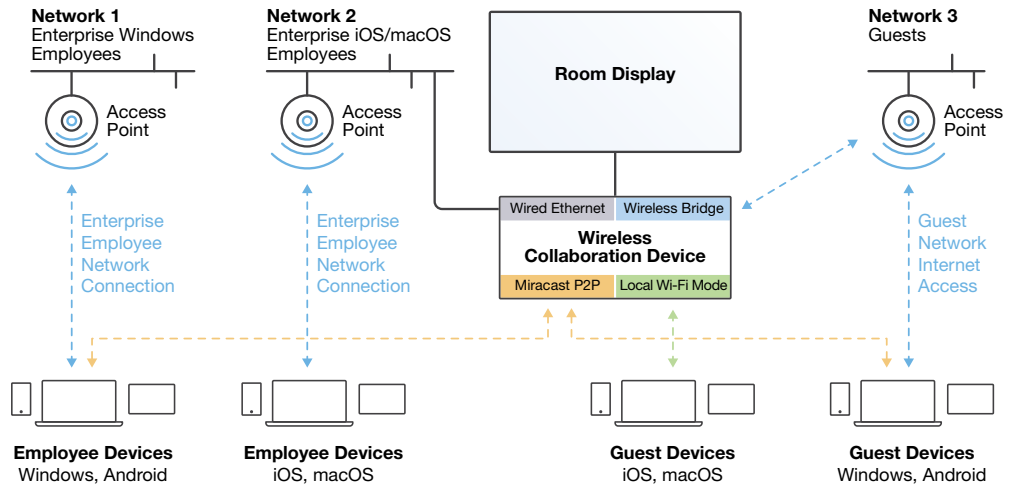
Essentially, all constraints for security, network, management and user deployment are met. No apps or USB dongles are used, no added training is required, and users of all major operating systems can be accommodated. Simultaneous network access is enabled for employees and guests. Management of the device's bands, channels and power for Miracast P2P AGO ensures optimal user experience and co-existence with existing nearby enterprise Wi-Fi access points. Touch screens are supported when available.

A disadvantage of the system above is if Bonjour broadcast is blocked on a network and cannot be cached out-of-band at the Wi-Fi access points. Such networks cannot support iOS/macOS screen mirroring device discovery and must trade off guest Apple access with employee Apple access.

Guest and Enterprise Network Isolation with Apple Isolation

Enterprises desiring wireless collaboration on guest and enterprise networks simultaneously often require separation of Apple devices from other devices due to Bonjour broadcasts. Isolation requirements for employee enterprise network access alongside guest networks compounds this problem.

There are essentially no wireless collaboration devices on the market that can provide this many simultaneous connections with network isolation. Until now.



In this example configuration, the device provides:

- Miracast P2P for guest or employee users via P2P wireless, plus simultaneous employee network access isolated from guest network Internet access
- iOS/macOS Screen Mirroring for employees via a separate employee network connected to the second device network interface with employee network access
- iOS/macOS Screen Mirroring for guests via local Wi-Fi mode with guest network Internet access through the device's wireless bridge
- Touch screen for Windows 10 Miracast users via USB to the display
- Easy on-screen instructions for connecting via either protocol

All constraints for security, network, management and user deployment are met. No apps or USB dongles are used, no added training is required, and users of all major operating systems can be accommodated. Simultaneous network access is enabled for employees and guests no matter what device is used.

Management of the device's bands, channels and power for Miracast P2P AGO and device local Wi-Fi ensures optimal user experience and co-existence with existing nearby enterprise Wi-Fi access points. Touch screens are supported when available. Bonjour traffic is fully sequestered with no compromises.



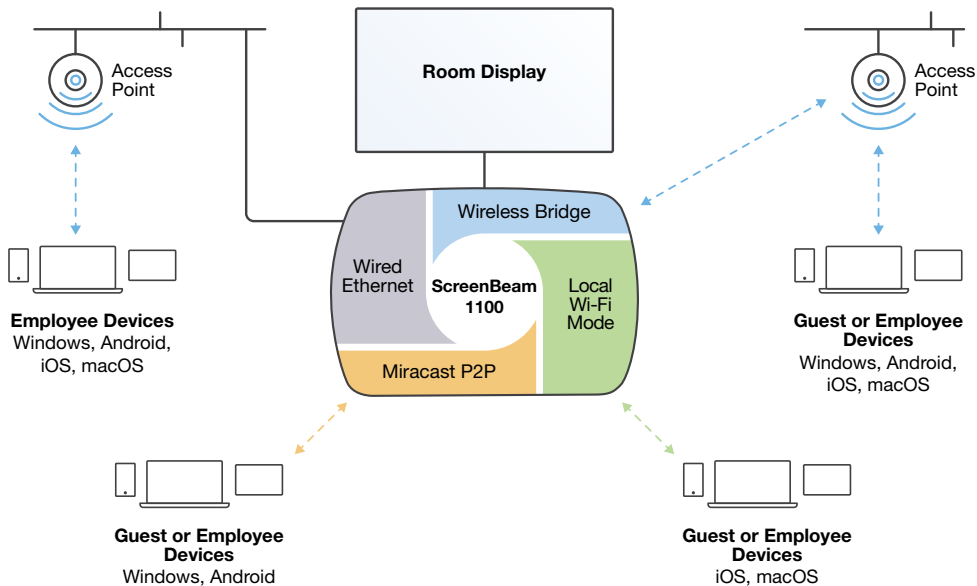
The key disadvantage of this system is that there are essentially no wireless collaboration devices on the market that can provide this many simultaneous connections with network isolation. Until now.

No-Compromises Wireless Collaboration

The ability to provide cost-effective centrally-managed wireless collaboration with built-in Miracast using P2P and Infrastructure, iOS/macOS screen mirroring, dual network interfaces and local Wi-Fi in a no-apps, no-dongles, no-wires 4K device with touch support has been sought after in professional AV for many years. ScreenBeam 1100 is the world's first solution to achieve this elusive goal.

ScreenBeam 1100's dual infrastructure network interfaces using wired Ethernet and dedicated 2x2 MIMO Wi-Fi provide simultaneous access to guest and employee networks, while an additional dedicated 3X3 MIMO Wi-Fi provides exceptional Miracast P2P AGO mode and local Wi-Fi mode access point performance for 4K. Wireless interfaces allow individual control of band, channel and power, ensuring optimal spectrum use and ease of deployment in dense wireless environments. ScreenBeam's Central Management System (CMS) allows easy provisioning, monitoring and upgrade in large-scale deployments. ScreenBeam 1100 enables ultimate enterprise deployment flexibility and security from full network isolation to full network integration in any meeting space.

With ScreenBeam 1100, the professional AV industry finally has a managed wireless collaboration solution at an unbeatable value.



Wireless collaboration would not be possible without native Miracast and iOS/macOS screen mirroring. As Microsoft's co-engineering partner on Miracast in Windows, including Windows 10 touch support and protected content playback, ScreenBeam 1100 is the premium solution for Miracast in the market. This expertise has evolved to include iOS/macOS screen mirroring for a true no apps, no dongles, no wires experience with native extended desktop support. Touch collaboration on Windows 10 devices provides seamless annotation for Office 365 applications so document annotations can be integrated and searched after a collaboration session. ScreenBeam 1100 increases productivity, reduces training and support costs, and integrates with touch screens for unparalleled collaboration capability.

With ScreenBeam 1100, the professional AV industry finally has a managed wireless collaboration solution at an unbeatable value. For more information about ScreenBeam 1100, please visit www.screenbeam.com.

white paper



IndustryLeader

ScreenBeam Inc., a leading wireless display and collaboration provider, delivers an app-free screen sharing experience on any modern device to bring intuitive wireless collaboration into any meeting space or classroom. ScreenBeam is Microsoft's co-engineering partner for wireless display enabling wireless Office 365 experiences.

ScreenBeam solutions are used as the validation platform for wireless display functionality by companies like Microsoft and leading PC OEM and device companies. Headquartered in Santa Clara, CA, ScreenBeam has offices across the United States, Europe and Asia.

ScreenBeam®

screenbeam.com

© 2019 All rights reserved. ScreenBeam and the ScreenBeam logo are registered trademarks owned by ScreenBeam Inc. All other names are properties of their respective owners. Specifications subject to change without notice. 091019