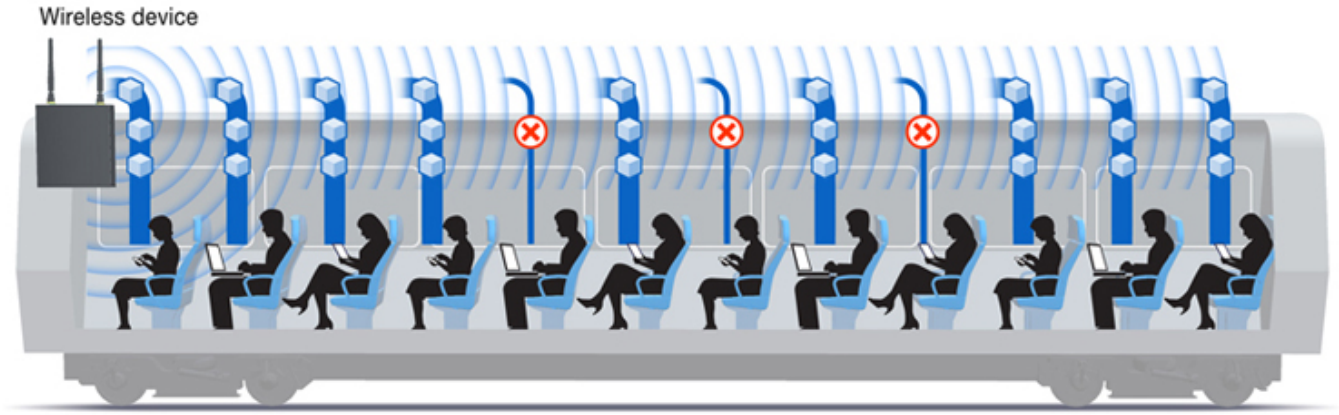
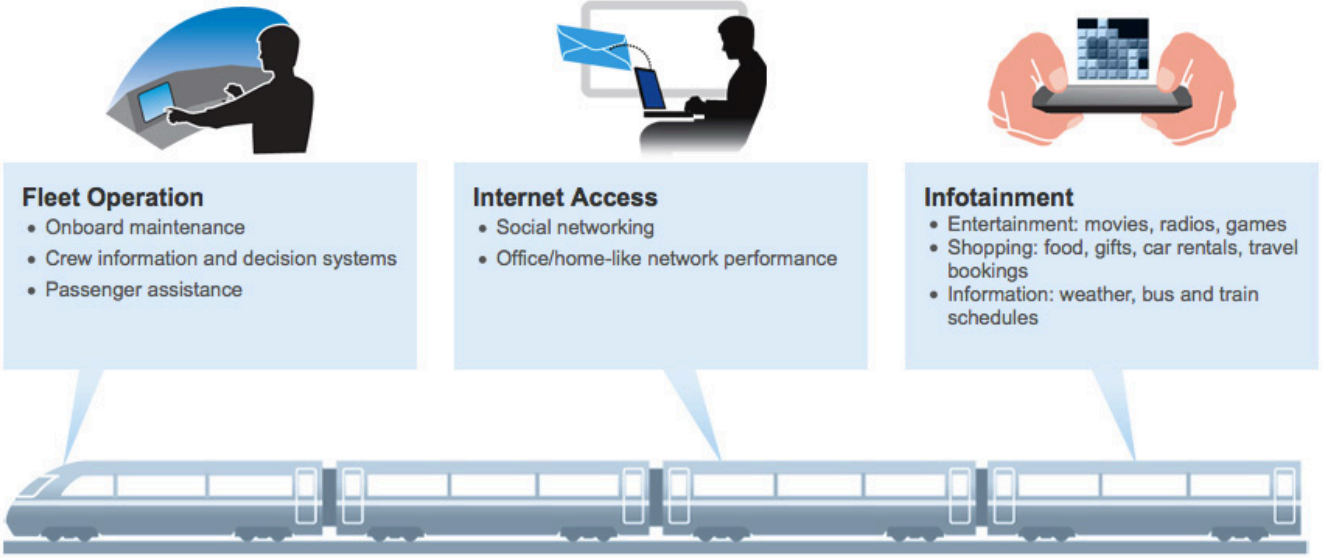
Passenger WI-FI

A Smooth Wi-Fi Experience is a Must for Increasing Infotainment Demands



With rail passengers demanding an Internet connection that is smooth enough to quickly search for information, view videos online, and connect to their company´s online data, it is more essential than ever for rail operators to provide a stable onboard Wi-Fi network. An unstable or difficult to access Wi-Fi connection will leave passengers with a bad impression of the service offered by the rail company, and have a decidedly negative effect on their overall travel experience.

What Can You Do with an Onboard Wi-Fi Network?

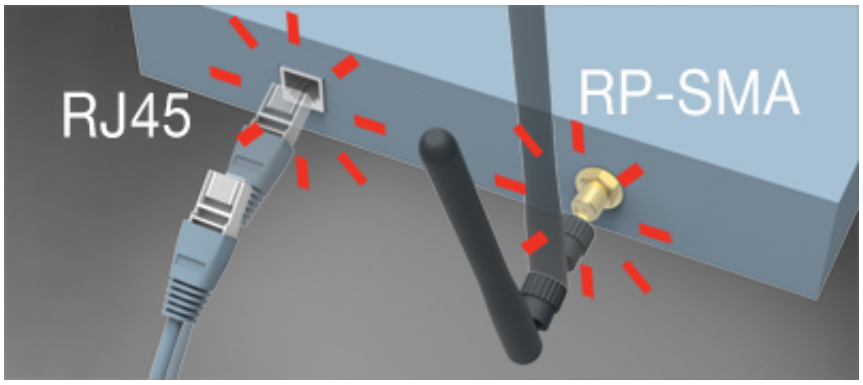


Delivering smooth Wi-Fi access is critical for onboard rail networks. Onboard environments have limited space and are prone to severe vibrations, making it more difficult to design a good Wi-Fi network, and requiring wireless devices tailor-made to ensure system stability. In addition, wireless devices that are used onboard must be able to ensure that every passenger has enough bandwidth and secure network access, without having to worry about being hacked.

Challenges for Constructing a Smooth Wi-Fi Experience

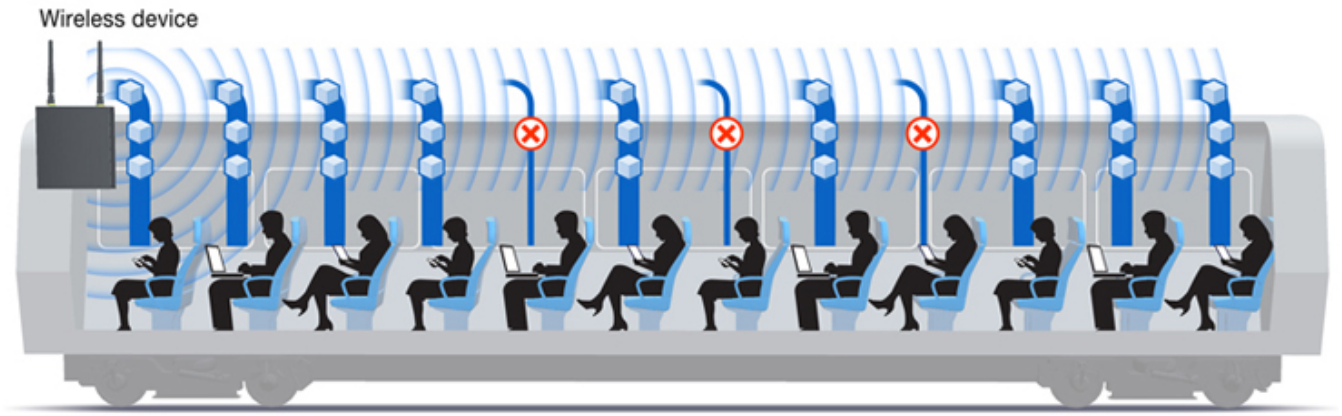
Four critical challenges need to be solved to offer a smooth Wi-Fi experience:

Equipment used onboard a moving train must be resistant to shocks and vibrations to ensure continuous system operation. For wireless devices, the antenna and Ethernet port are the main portholes for delivering Internet access to passengers and connecting with back-end systems. A rugged design is essential to prevent the antenna and Ethernet cable from getting disconnected, which would cause a sudden interruption in network access.



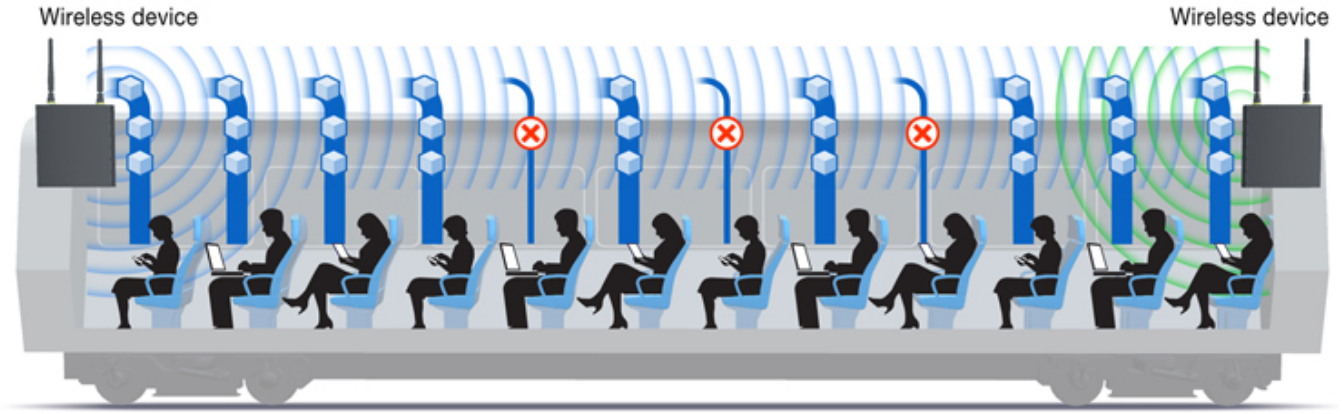
Unstable Connectivity in High Density Environments

On high-density trains, each car can seat hundreds of passengers, most of whom are expecting Internet access to read emails or watch online videos. In order to make the proper bandwidth calculations and optimize performance, onboard network designers need to know what kind of applications passengers are accustomed to using over the Internet to eliminate the possibility that any of the train´s passengers will be bothered by unstable Internet access.



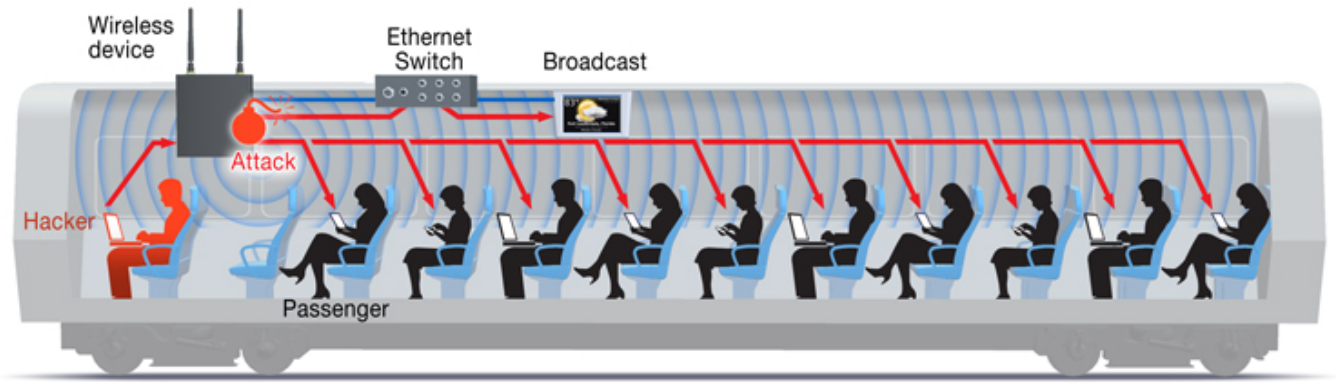
Don´t Get Overloaded with a Single Access Point

Two wireless access points installed in a single carriage can provide sufficient bandwidth for all passengers. However, without a proper network design, passengers? mobile devices congregating in a carriage will connect to a particular AP in the area, causing slow connections or even no connection for some passengers and leaving other APs with light loads.



Public Wi-Fi Hotspot

Any device that connects to onboard APs belongs to the same network with onboard systems such as broadcast and other control systems. Public network environments must be protected from hackers to ensure the safety of onboard systems connected to the same network topology, as well as the privacy of passengers who access the train´s Wi-Fi APs.



Tailor-Made AWK-RCC Series Wi-Fi Devices Ensure the Best User Experience

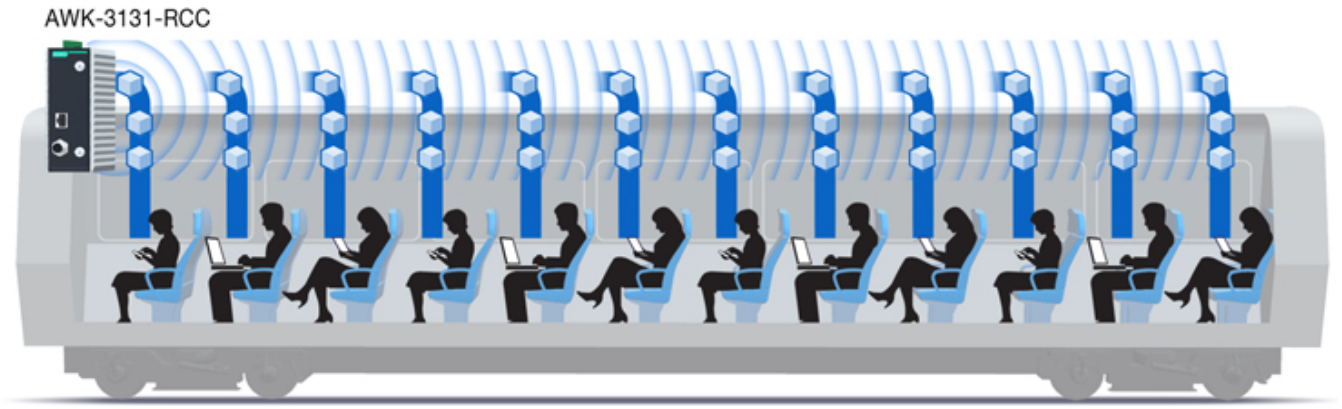
Moxa?s AWK-RCC series devices are tailor-made for onboard Internet access and to provide fast and secure hotspots for passengers on trains. The benefits of the AWK-RCC series includes:

Best Design for Onboard Applications

The AWK-RCC series has built-in M12 connectors to ensure that onboard networks stay connected and QMA ports deliver continuous Internet access under the constant vibration and shock common in onboard environments.

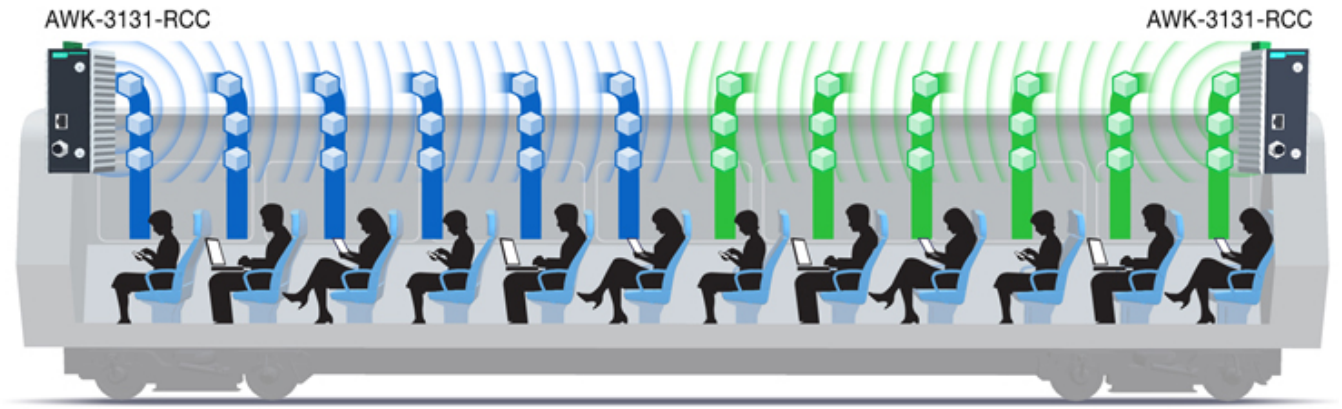
Stable and Concurrent Wi-Fi Access

To ensure stable Internet access in high density environments, the AWK-RCC series has been optimized and tested to achieve up to 60 links from a single device, letting each of these 60 passengers enjoy stable Internet access, at the same time.



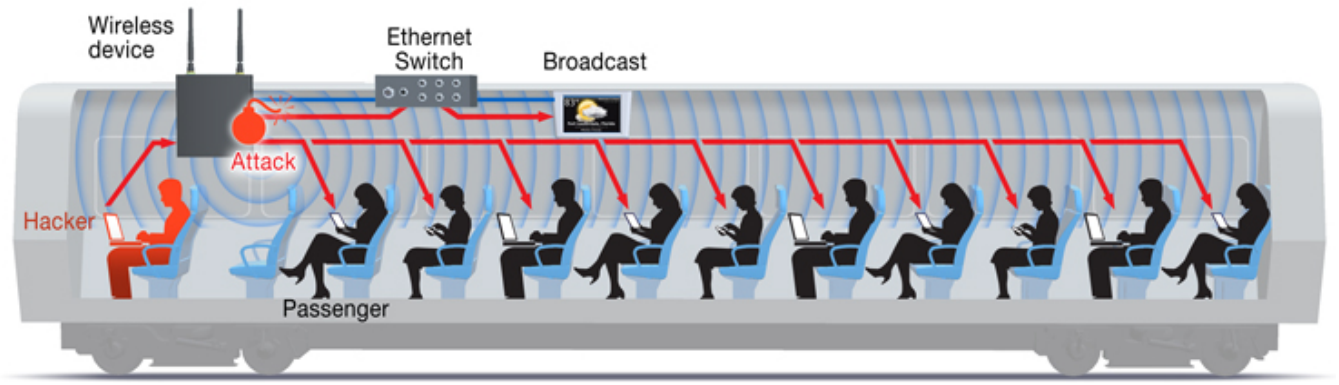
Even Bandwidth Distribution for all APs

To provide maximum bandwidth for all onboard mobile devices and enable even distribution of these devices in a high-density environment, the AWK-RCC series supports an effective client load balancing feature that distributes bandwidth evenly for all passengers.



Secure Wi-Fi Access

The AWK-RCC series supports wireless client isolation to prevent both on-board systems and passenger´s mobile deceives from directly communicating with each other on the same network. This provides an added layer of protection against passengers gaining access to other devices for malicious purposes.


Wireless device
Ethernet Switch
Broadcast
Attack
Hacker
Passenger