CPE Plays Major Role in Integrating Broadband Access, Wireless Connectivity and Security to Maximize 5G FWA for Connected Homes

Thibaud Lepage,
Director of Product Management for 5G Fixed Wireless Access, Technicolor Connected Home

The introduction of 5G fixed wireless access (FWA) services to the home has introduced an exciting new broadband option for both network service providers and consumers. Long-term success, however, will require network service providers (NSPs) to carefully integrate broadband access, in-home wireless connectivity and rigorous security measures.

To better understand how these factors can be managed by a strategic approach to the design, development and deployment of carrier-class 5G FWA customer premises equipment (CPE), we caught up with Thibaud Lepage, Director of Product Management for 5G FWA at Technicolor Connected Home.

Here is what he had to say:

5G fixed wireless access (FWA) will play a key role in defining the connected home of tomorrow. It is an exciting time for both consumers and network service providers (NSPs). We expect a new generation of 5G home gateways to bridge technology gaps that have existed in some segments of the market. It will offer high-speed connectivity to subscribers that have — until now — been left out of the full broadband experience in their homes. NSPs are exploring how they can fully take advantage of 5G fixed wireless connectivity.

It is, however, an opportunity that requires careful thinking. Simply supplying 5G FWA to the home will not address the ability to offer broadband connectivity throughout the home to provide access to multiple devices and users. Delivering 5G to a room is one matter, but delivery is irrelevant if fast broadband cannot be distributed effectively to every device and user in the home.

To maintain high-performance NSPs will have to deploy gateways that are of carrier-grade quality. Technicolor gateways based on HOMEWARE and RDK-B technology leverage open systems. This is the key to providing reliable and managed middleware that enables NSPs to tap into a thriving ecosystem of partners who can bring innovative services to subscribers.

Technicolor Connected Home's HOMEWARE offerings are based on open value-added standards, which our engineers have extended to be carrier-grade. RDK-B is a fully customizable open-source software solution that standardizes core functions using broadband. This approach enables our NSP clients to add applications to the gateway in much the same way consumers can add apps on smartphones.

At Technicolor Connected Home, we can pre-integrate applications from our partners' apps via the Technicolor HERO program and deliver complete life cycle management of those apps while improving how they are serviced — including upgrades and maintenance — all within the gateway.

For instance, our gateways are EasyMesh-enabled, and our partnerships with Airties and Plume make Wi-Fi roaming seamless throughout the connected home no matter how many devices or users are in play. In addition, we also offer a range of extremely fast Wi-Fi repeaters and extenders to deliver the truly connected home of the future.

Security is a Top Priority

The past two years have seen consumers around the world become even more dependent on connectivity in the home. This has generated a tremendous amount of sensitive data that is shared across devices and cloud services. This means that security must be a top priority.

Customer premises equipment (CPE) from Technicolor Connected Home has always been designed with this priority in mind. We are committed to protecting personal data, privacy and access to home network devices from piracy and network attacks.

5G FWA CPE, just like any other CPE, is no exception. We have rigorous security measures to handle broadband 5G FWA access to the home, and integrated protection measures through the hand-off to devices that enable wireless connectivity within the home. This allows NSPs to protect a wide range of offerings — from entertainment services to IoT devices. Technicolor embraces a rigorous three-step security check to ensure that our device middleware and the applications running on it are protected.

Step 1: Every time code is contributed to the development of our products, it is verified overnight for security vulnerabilities. Developers are automatically notified — during validation and before it is delivered to NSP customers.

Step 2: Once the code is comprehensively validated by a dedicated security team in both open box (via code reviews) and closed box (via penetration testing). A dedicated team tracks software components and technology to continuously conduct security checks to assess risk even after our products are delivered. At regular intervals, independent third-party security labs validate the products.

Step 3: The final step is to verify the performance of our products in real-life operation, in the real environment. We have invested in rigorous testing facilities to ensure that our CPE offerings are secure, interoperable and app-ready.

We have developed a dedicated software development kit (SDK) for our gateways that allow our NSP clients to bring new services to market and improve average revenue per user (ARPU) performance through integrated software applications.