A New Approach to Delivering Secure Community Wi-Fi

Deploying Cloud-Based WPA2 for Residential Hotspots

Table of Contents

Executive summary 1
Trends in Wi-Fi service. 1
Challenges in securing Wi-Fi 2
Cloud-based WPA2 architecture 2
Advantages of cloud-based WPA2 . . . 4
Proof of concept and lab trials 4
New business models and services . . 8
Conclusion 8

Executive summary

Community Wi-Fi, and also public Wi-Fi, have become key strategies for customer retention and growth for service providers in many regions. Not only does it give customers more pervasive connectivity, it also opens the door for new business models and services based on wholesale Wi-Fi. This is especially relevant with the rollout of 5G, when carriers are expected to provide much larger capacity by deploying many more small cells and hotspots. Residential hotspots, or "homespots," offer an efficient way to provide community Wi-Fi using existing infrastructure. However, securing the internet access of community users over the huge installed base of legacy access points and home gateways is a challenge for operators and also a concern for the community users. It is even more difficult in homes that have distributed multiroom access points or range extenders that are physically separated from the home gateway.

Cloud-based Wi-Fi Protected Access (WPA2) moves certain security functions from the customer premises equipment (CPE) access point system to the cloud to enable end-to-end secured internet connectivity. It works across any type of legacy network, CPE system, client device, and client operating system (OS), with no impact on throughput and latency.

Intel, Telenet, and ARRIS have developed a unique way to implement cloud-based WPA2 and conducted lab trials to demonstrate its benefits. These trials prove the feasibility of virtualizing residential Wi-Fi access point functions and provide a scalable path for secure internet access for community Wi-Fi users.

Trends in Wi-Fi service

Today, Wi-Fi service providers are under pressure to manage an increasingly complex technology environment while responding to new expectations for performance. Customers want seamless connectivity throughout the home, as well as the option to take advantage of services once they leave their homes by connecting to community Wi-Fi.

Additional access points that are being placed throughout homes present a new opportunity to expand community Wi-Fi in dense urban environments. This is an especially critical area of business for cable operators, allowing them to follow customers outside the home.

To deliver community Wi-Fi, service providers broadcast both private and public Wi-Fi service set identifiers (SSIDs) from residential access points. Currently, some 100 million residential access points are operating public Wi-Fi network SSIDs while also delivering home connectivity.

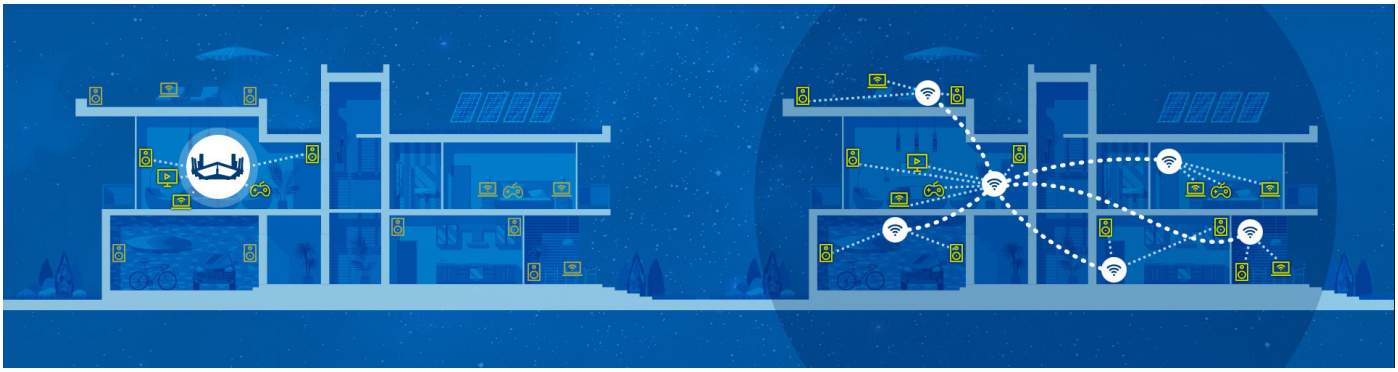


Figure 1. The home network topology is evolving to a home network with multiple access points and extenders with wired or Wi-Fi backhaul.

Challenges in securing Wi-Fi

While it's clear that a home network with multiple access points and extenders is advantageous for coverage throughout the home as well as delivering community Wi-Fi, this setup is vulnerable to security breaches. Because WPA2 terminates at the range extender or access point, and therefore protects only the link between the clients and access point or range extender, traffic from the extender to the gateway is exposed to viewing from the private network.

When broadcasting both a private and public SSID from a residential access point, service providers must separate and protect public traffic from private traffic (and vice versa) across all legacy network types and devices and also ensure private users can't inspect public traffic going over their local network.

Because residential networks are not designed with the same trustable security measures as are common in enterprise networks, nor are they located in trusted locations from the community perspective, service providers must take a new approach to delivering protected Wi-Fi access.

Cloud-based WPA2 architecture

Drawing from combined industry expertise, Intel, Telenet, and ARRIS have developed a cloud-based WPA2 architecture to enable secure Wi-Fi access for any client over multivendor, multigeneration home networks. The result is the ability to deliver end-to-end security for community Wi-Fi.

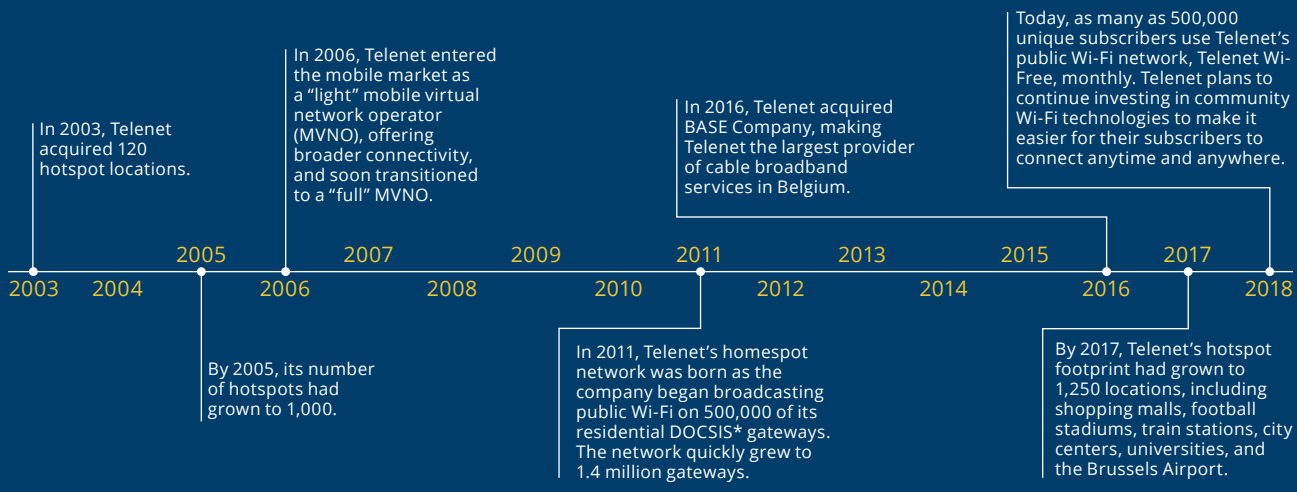
Architecture summary

With traditional Wi-Fi architectures, a single access point handles all functions, including security, client management, and resource management.

With cloud-based WPA2, the functions related to client Wi-Fi security are moved from the access point to the cloud. All control functions are established with a secure connection to the cloud. A community Wi-Fi data frame flows unmodified between clients connected to homespots and the service provider core network, where at both ends it undergoes WPA2 encryption and decryption.

Telenet: Mapping a path to community Wi-Fi

To provide customers with seamless, hassle-free connectivity, Telenet has deployed one of the largest Wi-Fi networks across Belgium. In building its hotspot and homespot networks, Telenet has emphasized ease of use, simplified onboarding, and security. Devices can automatically connect and authenticate to Telenet's public Wi-Fi network, so the user does not need to enter credentials every time. Additionally, the wireless connection between the client and network is encrypted via Wi-Fi Protected Access II (WPA2).



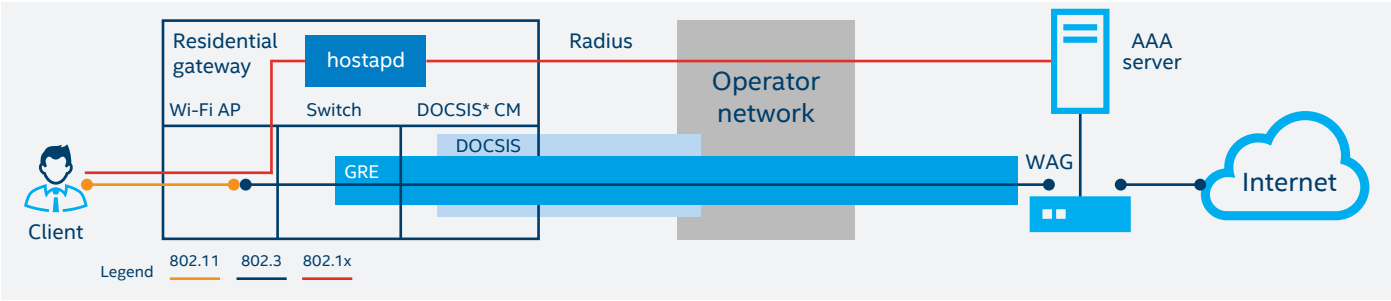


Figure 2. Existing community Wi-Fi architecture

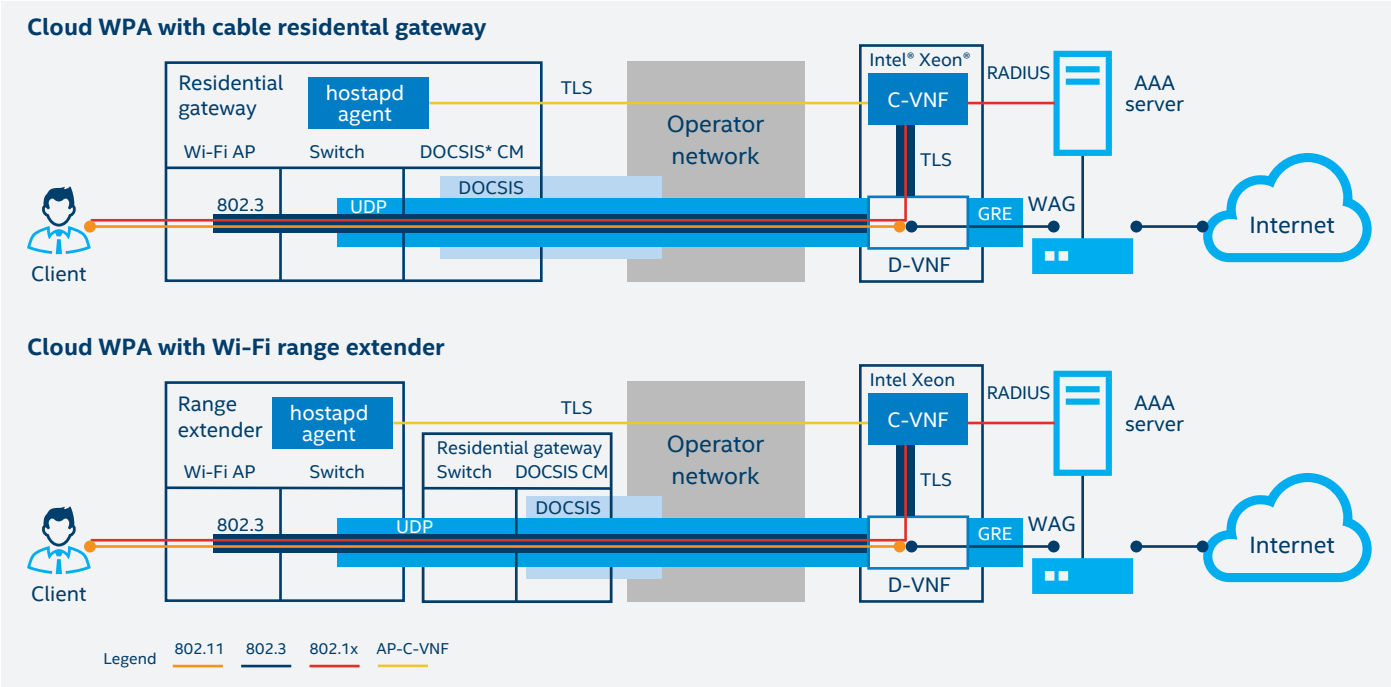


Figure 3. Cloud WPA2 community Wi-Fi architecture

Functional partitioning

Cloud-based WPA2 splits the functionality of the access point between the homespot and virtual network functions (VNFs) on the service provider core network.

1. A client device on the community Wi-Fi SSID sends WPA2-encrypted 802.11 packets to the residential access point. The access point is configured to pass through all data traffic that belongs to the community Wi-Fi SSID.
2. 802.11 data packets are not treated for encryption or decryption by the access point. Instead, they are passed unmodified to a corresponding WPA2 data VNF in the service provider network. This VNF performs WPA2 encryption and decryption of client data and converts data traffic between 802.11 and 802.3 protocol formats.
3. The WPA2 data VNF then passes traffic to the service provider's wireless access gateway (WAG).

The handling of the initial connection (802.11 authentication and association) for the community Wi-Fi SSID is left in the access point. Remote Authentication Dial-In User Service (RADIUS) client and secured connection establishment logic (authenticator and four-way handshake) is moved to the service provider core network as another VNF (WPA2 control VNF).

1. The WPA2 control VNF obtains a master session key (MSK) for the Wi-Fi client as a result of 802.1x authentication protocol exchange and derives WPA2 pairwise and group keys (PTK and GTK).
2. The WPA2 control VNF configures PTK and GTK to the WPA2 data VNF to be used for encryption and decryption.

Protocols for communication

For such a partition to work, protocols were defined for communication between the residential access point system, the WPA2 data VNF, and the WPA2 control VNF.

- The interface between the access point and WPA2 control VNF is encapsulated in the TLS connection that is established between every community Wi-Fi basic SSID (BSSID) and WPA2 control VNF. In its most basic form, it carries over indications from the community Wi-Fi BSSID that a basic service set (BSS) has been activated, and the client has been associated or disconnected.
- The WPA2 control VNF notifies the community Wi-Fi BSS that a specific client has established a WPA2 secured connection or has to be disconnected.

- The interface between the WPA2 control VNF and WPA2 data VNF is encapsulated in the TLS connection that is established between both VNFs. Over this connection, the WPA2 control VNF notifies the WPA2 data VNF that a specific BSS has been activated, and a client has been added or removed from the BSS. The connection between VNFs is used to configure GTK for the BSS or PTK for a specific Wi-Fi client.

Communication between the access point and WPA2 data VNF is carried over an IP-based encapsulation tunnel set up between these entities, which could be GRE, UDP, or another type of tunnel, depending on the needs and requirements of the deployment.

- 802.11 data packets received from the client are encapsulated over the IP tunnel and sent to the end point terminated at the WPA2 data VNF. The data VNF decrypts received 802.11 data packets and prepares them to be transmitted to the WAG.
- The data VNF receives data traffic for the client from the WAG, converts it to the 802.11 format, and performs WPA2 encryption. The packets are then sent to the access point encapsulated in the IP tunnel for transmission to the client.

Comparison of network architectures to deliver secure internet access over Wi-Fi

Enterprises may use a combination of Datagram Transport Layer Security (DTLS), internet protocol security (IPSEC), and Media Access Control Security (MACsec) to create encrypted tunnels for secure Wi-Fi. However, the use of residential access points presents unique challenges:

- Public hotspots are assumed in untrusted locations with unknown backhaul to their core network.
- DTLS, IPSEC, and MACsec are rarely supported on cost-sensitive residential CPE already in the field, especially for speeds of 100s Mbps.
- Protecting against man-in-the-middle attacks with consumer switches, routers, or access points between the service provider's CPEs is difficult, or impossible.
- Often, the only common ground for client capabilities is that they are Wi-Fi certified.

In contrast to IT-controlled environments, the strategies for securing Wi-Fi based on residential access points are limited. Cloud-based WPA2 can provide a very good solution when compared with other techniques:

- **WPA2 between Wi-Fi access points in the home.** WPA2 is considered a secure-enough solution for Wi-Fi communication and provides protection without affecting throughput or latency. However, to break the protection across the home, the adversary needs only to add a wire interface between one of the home's access points and the broadband gateway.
- **Tunnels between two nodes in the home, or between nodes in the home and the cloud.** High-speed IPSEC, DTLS, or MACsec are rarely supported by residential equipment and would most often require CPE to be replaced. Furthermore, by controlling one of the access points in the home, an adversary could still create a man-in-the-middle attack.
- **A VPN tunnel between clients and a VPN server on the service provider's core network.** End-to-end VPN is a good way to secure community traffic over any residential network. The main disadvantage is the impact on performance. It takes significant client CPU and battery resources to preserve internet speeds while encrypting all packets by the VPN application.
- **Cloud-based WPA2.** Like VPN, cloud-based WPA2 secures traffic over any residential network. Unlike VPN, the encryption function of the client is native WPA2, so speed is not impacted by the client device's capabilities to accelerate the VPN application.

Advantages of cloud-based WPA2

The cloud-based WPA2 architecture demonstrated by Intel, Telenet, and ARRIS offers service providers a wide range of benefits:

- Secure Wi-Fi protection with no impact on internet speed or latency.
- Support for any Wi-Fi client device and OS with no need to install a VPN, resulting in internet speeds that are as fast as before because no change is made on the client when the access is secured.
- Deployment over legacy home networks with no new installation of CPEs (access points, switches, or gateways).
- A cost-effective solution that doesn't need to be planned for peak usage, but to the average utilization because WPA2 capacity in the cloud is shared across many homes.
- Updates that can be made without having to patch the CPE, resulting in greater operational efficiency.

Proof of concept and lab trials

To present a complete value chain for cloud-based WPA2, Intel, Telenet, and ARRIS conducted lab trials across three sites to test the concept. The goals of the lab trials were to:

- Validate the cloud-based WPA2 architecture for community Wi-Fi
- Confirm there is no impact on user experience for devices running on Windows*, Android*, and iOS* using popular applications
- Measure the impact on the Wi-Fi client connection success rate under variable network delays
- Measure WPA2 data VNF performance under various traffic load conditions
- Measure Cloud WPA2 vs. VPN tunnels in terms of CPU utilization and utilization on the client device
- Measure the maximum distance between the WPA client and the WPA VNFs

Summary of the lab trial results

The results of the lab trials confirmed the security and performance advantages of cloud-based WPA2 architecture. Among the key results achieved:

- 100 Mbps[1] throughput on Wi-Fi clients
- Consistent performance regardless of OS (Windows® 10, Android, and iOS)
- Smooth live video chat with no impact to user experience
- Server performance of 8 Gbps per core for large packets with AES-NI Cryptodev implementation in DPDK
- Significant advantages in client CPU utilization compared with end-to-end VPN
- Resiliency over huge geographical distance (between client and WPA2 server)

Three sets of tests with various network configurations were run at Telenet, ARRIS, and Intel, which accounts for the differences in measured performance below. More details can be found at 01.org.

Measured performance	Intel site	Telenet site	ARRIS site
Highest throughput to client[2]	Iperf UDP 1500B packets: 140 Mbps downlink, 92 Mbps uplink	Speed test, MSS1350B: 101 Mbps downlink, 17 Mbps uplink	iperf TCP, MSS 1350B: 135 Mbps downlink, 100 Mbps uplink
Smooth user experience with popular apps	YouTube*, Amazon Prime*, WhatsApp* video call, Skype*, Facebook*, Instagram*	YouTube, Netflix*, WhatsApp video call	YouTube, WhatsApp video call
100 percent successful connection establishment at variable simulated transmission delay	Range: 0–200 milliseconds	Not tested	50 milliseconds

The lab trials showed it is possible to overcome concerns regarding the complexity and availability of support by residential CPE present with alternative solutions, such as IPsec and MACsec, as well as performance concerns present with VPN. The following sections summarize server, delay, and CPU load benchmark results. A detailed report of Cloud WPA2 POC testing across the three lab sites is available at 01.org.

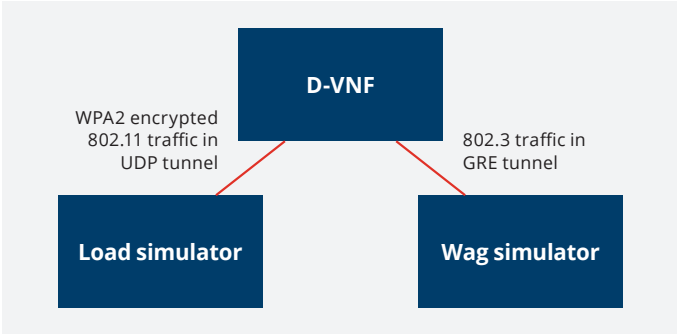


Figure 4. Conceptual test setup

Cloud WPA2 data VNF performance results

Cloud Wi-Fi data VNF server testing configuration:

Hardware overview

- Hardware: Intel® Xeon® Processor E5-2699 v3, 2.30GHz, 18C Dual Processor; Intel® Ethernet Server adapter X710 4 x 10G NIC; Intel DH895XCC QuickAssist Accelerator PCIe card AXXQAAPCIE
- Host OS: Fedora* 24, Linux* kernel v4.10
- Guest OS (VNF-D): Fedora 24, Linux kernel v4.5, DPDK v18.02, AES-NI MB v0.48, R-WPA VNF v18.03
- Intel® Virtualization Technology for Directed I/O (Intel® VT-d) used for network access from VMs

Application setup

- VNF-D: DPDK-based application using one physical core (with UL and DL on sibling hyperthreads)
- Performance tests with both Intel® AESNI-MB library and Intel® QuickAssist Technology (Intel® QAT) offload used for AES-CCMP encryption/decryption
- UDP tunneling on AP interface, GRE tunneling on WAG interface

Traffic characteristics

(uplink encapsulated size with crypto size in brackets)

1. Standard iMix: 54%:170B [64B], 38.5%:682B [576B], 7.5%:1606B [1500B]
2. Cable iMix: 15%:190B [84B], 10%:362B [256B], 75%:1386B [1280B]

Test methodology

- Performance results for bidirectional traffic (uplink and downlink)
- Uplink:downlink traffic ratio = 1:1 (aggregate traffic = 2x bidirectional traffic)
- Max throughput for zero packet loss
- Uplink traffic generated by DPDK Pktgen (user data frames only, fragmented when packet size is higher than 1500B)
- Downlink traffic generated by L2 loopback of uplink traffic through WAG simulator

Figure 5 shows the aggregate[3] throughput and packets per second for the R-WPA dataplane VNF for a sweep of fixed packet sizes under the two acceleration scenarios at zero packet loss. Numbers shown are totals, when adding the downstream and upstream rates. Throughput in both cases increases with packet size, although with different slopes, until the Intel QAT- accelerated scenario saturates the 10G link interface and both scenarios become affected by SARing[4] at 1492B packet size.

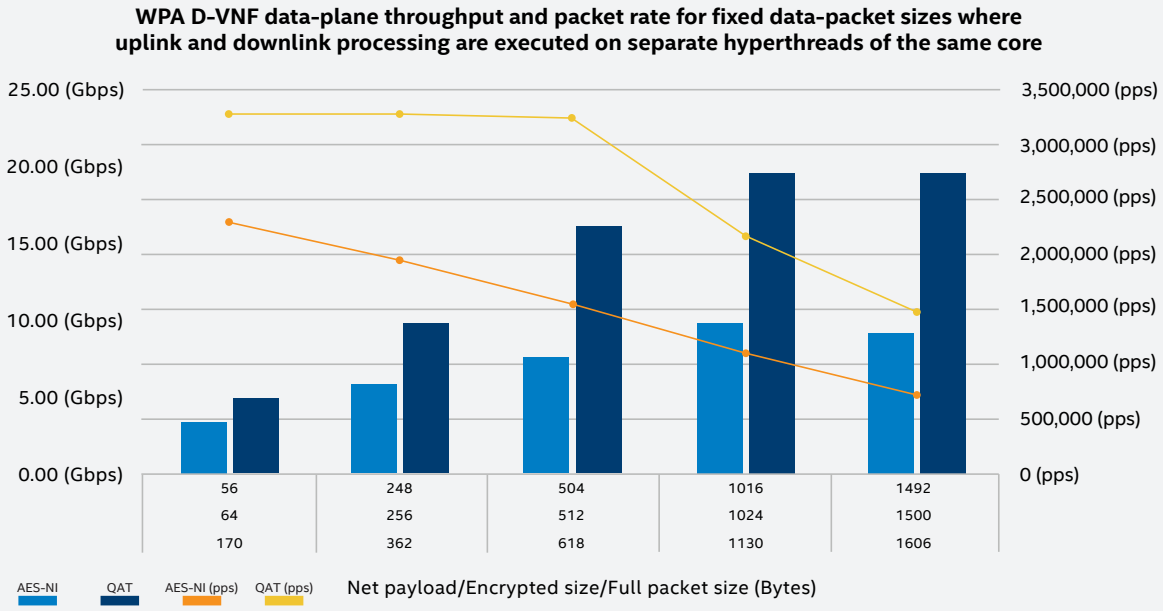


Figure 5. Single-core data-plane VNF performance for fixed packet sizes

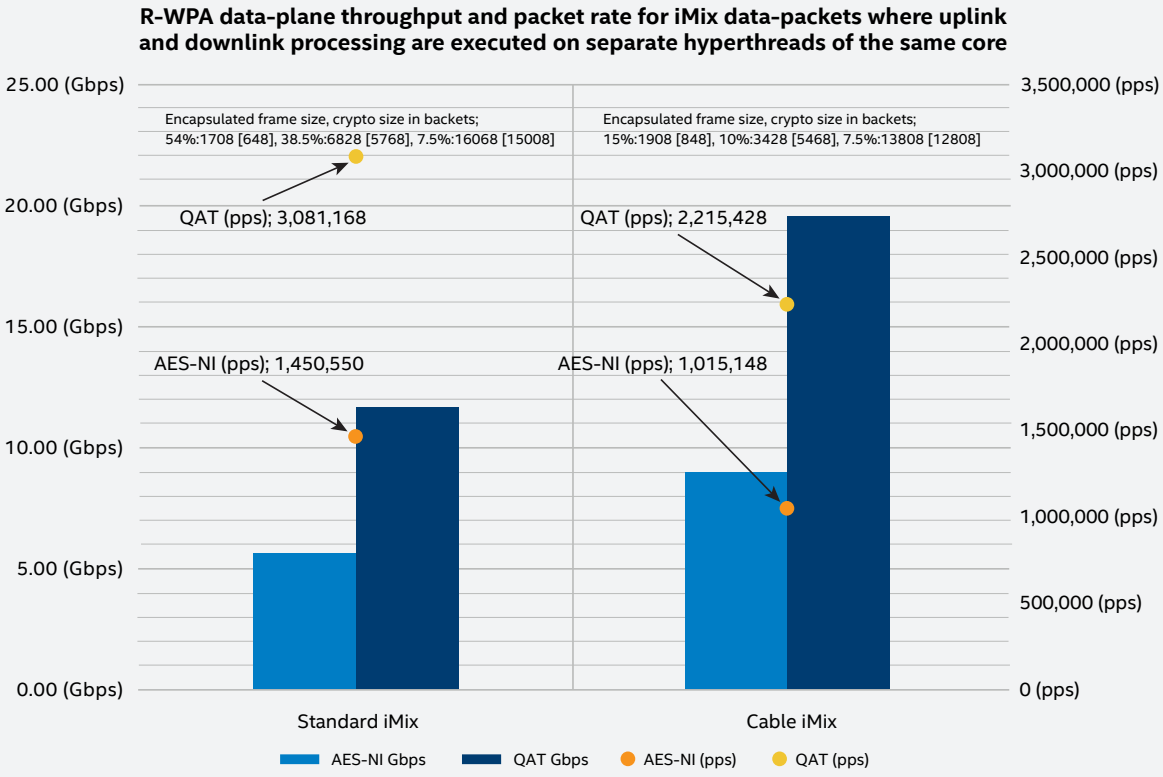


Figure 6. Single-core data-plane VNF performance for iMix packet size distribution

Impact of distance between Wi-Fi AP and server control and data VNF distance on client connection establishment time

Distance is represented by variable delay simulated by server software (Intel® Xeon® processor)

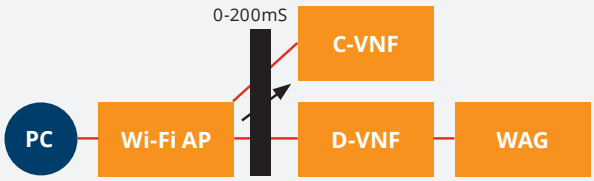


Figure 7. Conceptual test setup

Figure 8 shows that Cloud WPA VNFs could be deployed 1000s km from AP in a different country or even continent without user perceivable impact on connection time.

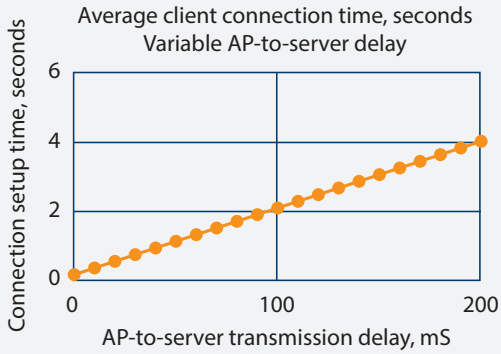


Figure 8. Connection time

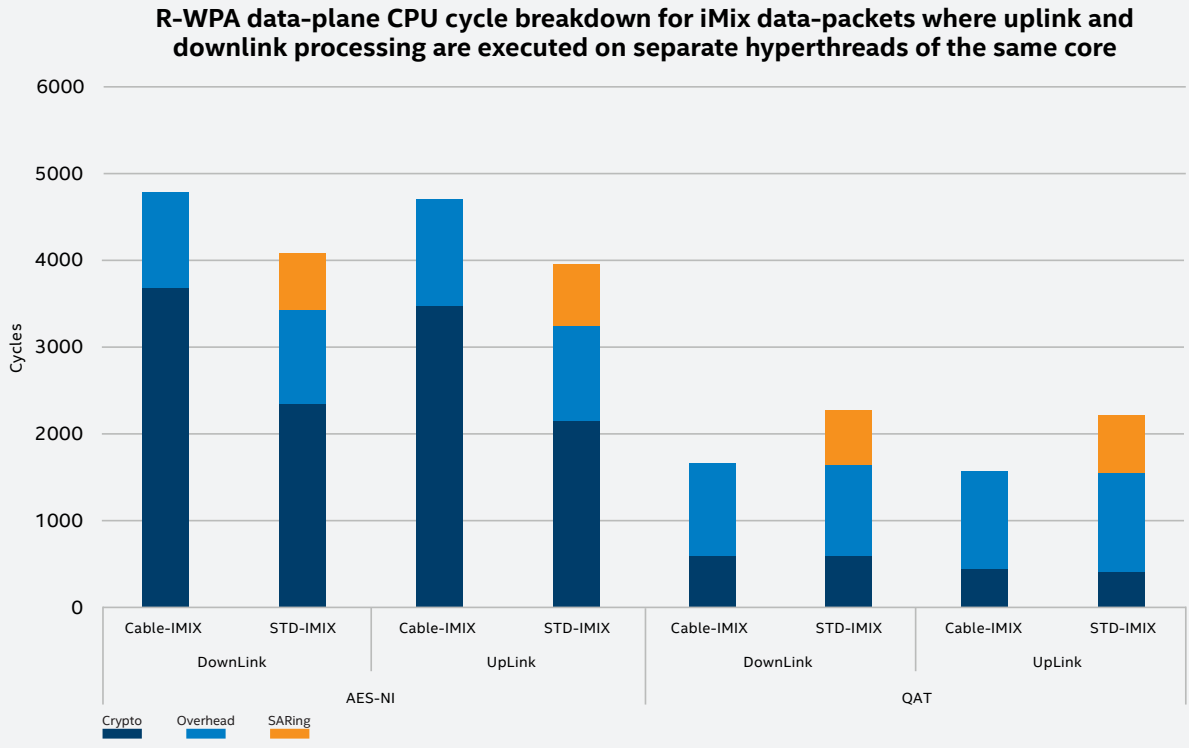


Figure 9. Breakdown of average cycle cost per packet for single-core data-plane VNF processing iMix data-packets

Figure 9 shows the average per-packet cost in CPU cycles for the uplink and downlink, where lower cycles correlate to better performance. The costs shown are broken into crypto and non-crypto costs (i.e., overhead for frame conversion processing).

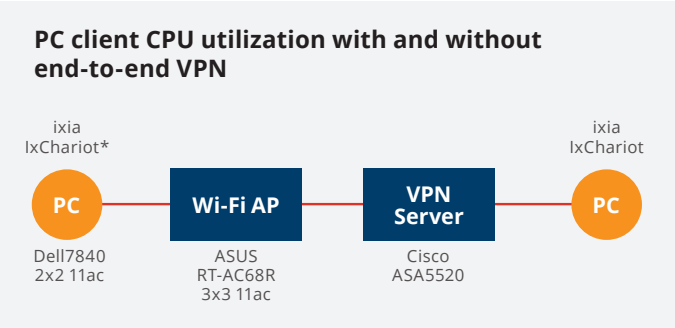


Figure 10. Conceptual test setup

PC under test configuration: Intel® Core™ i7processor -7600U@3.8GHz RAM 8GB 64-bit Windows 10 Enterprise. VPN Client SW: Cisco AnyConnect 4.4.03034. VPN connection parameters: SSL: DTLS, AES128-SHA1; IPSec: IKEv2, AES128-SHA1

Test methodology: Traffic generated with Chariot: UDP downlink, 1500B packet size. CPU load measured using Windows Task Manager

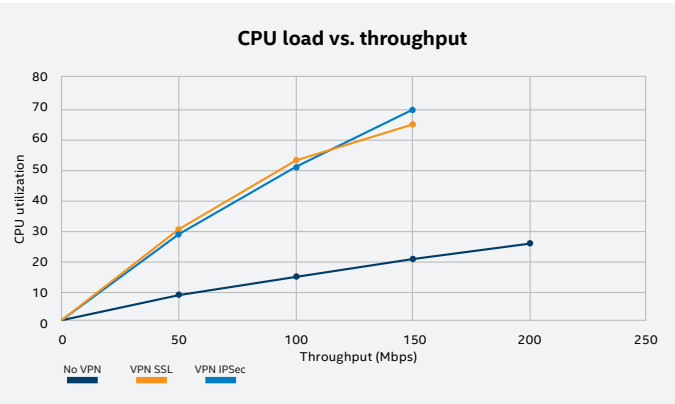


Figure 11. Performance advantage of WPA2 over client-based VPN

Figure 11 shows that Cloud WPA2 offers a performance advantage over client-based VPN since a smaller amount of client CPU and battery resources are required to preserve internet speeds.

New business models and services

By protecting access for nonresidential Wi-Fi users, cloud-based WPA2 architecture has the potential to be used in new business models and services. With a neutral host model, residential service providers from either the same country or different countries can share or lease Wi-Fi capacity with each other in a secure way. This expands the reach of any given service provider beyond their existing physical footprint. Combining neutral hosting with wireless home infrastructure may become an integral part of creating smart cities and virtual communities. By securely merging residential with municipal communication infrastructure, the industry can transform service provision and empower new secured IoT applications like smart meters and traffic signals.

Conclusion

Cloud-based WPA2 has the potential to become an integral part of designing home Wi-Fi, especially as community Wi-Fi grows more popular and more residential hotspots get deployed for 5G capacity needs. The architecture demonstrated in the lab trials can be deployed on legacy infrastructure with minor software changes and no additional hardware. It leverages efficient sharing of crypto resources without creating traffic detours across the internet and preserves performance in Wi-Fi connectivity. In addition, the low-intrusiveness character of cloud-based WPA2 makes it an appealing tool for adaptation in other Wi-Fi crypto methods like WPA3.

The true value of cloud-based WPA2 is unlocked when adopted over a large legacy-installed base of home networks. The proof of concept offers a first step toward the possibility of standardizing a secure, efficient, and scalable way to provide community Wi-Fi over residential homespots, as well as whole-home coverage. Service providers can replicate this proof of concept setup in their own labs, and solution providers can develop WPA2 VNF products based on this implementation.

Intel, Telenet, and ARRIS remain committed to addressing industry challenges such as security and contributing innovative Wi-Fi technologies that maximize the value of technology already used in the home and service provider infrastructure. There are numerous possibilities for cloud-based WPA2 to be used in smart cities and communities, as well as the new business opportunities in the communications industry.

1. 100 Mbps throughput is limited by POC implementation of pass-through mode on Wi-Fi AP platform; not optimized for performance data-path processing in Wi-Fi driver, Linux* Bridge, or UDP encapsulation Linux kernel module.
2. Uplink and downlink speeds are attributed to the connection performance between the access point and client.
3. Aggregate performance is 2x the unidirectional, as both downstream and upstream are run at the same data rate.
4. SARing (Segmentation and Reassembly): Segmentation (fragmentation) of downlink traffic when full packet size is >1500B. Reassembly of upstream packets that would have been fragmented at the Wi-Fi AP.

0418/CMD/LS/PDF 337543-001US