ANYFI GATEWAY SOFTWARE

HIGH-PERFORMANCE LINK LIBRARY EDITION

DATASHEET

KEY BENEFITS

- Unique SDWN architecture extends the SWw interface all the way to the Trusted WLAN Access Gateway *(TWAG)*, ensuring end-to-end security between mobile device and mobile core even in the case where the Wi-Fi access point cannot be trusted.
- Compatible with any Wi-Fi access point or residential gateway integrating Anyfi.net software – available to all OEMs no-charge and royalty free.
- ISO C link library – easy to integrate both in Intel DPDK and service routers based on network processing platforms such as Cavium.
- Traffic steering based on device MAC and IMSI ensures that all mobile core frame processing can be performed on a single processing card, in a single process, zero copy.
- Ready to support advanced telecom requirements such as resiliency.
- No dependencies on third party or system libraries.

KEY PERFORMANCE METRICS

- Up to 40 Gbps IEEE 802.11 CCMP *(AES128 encryption/decryption with integrity check)* on single Intel Dual Xeon E5 system with AES-NI.
- SDWN architecture with just-in-time resource allocation means no resources allocated until mobile device actually connects – infinite scalability in number of access points.

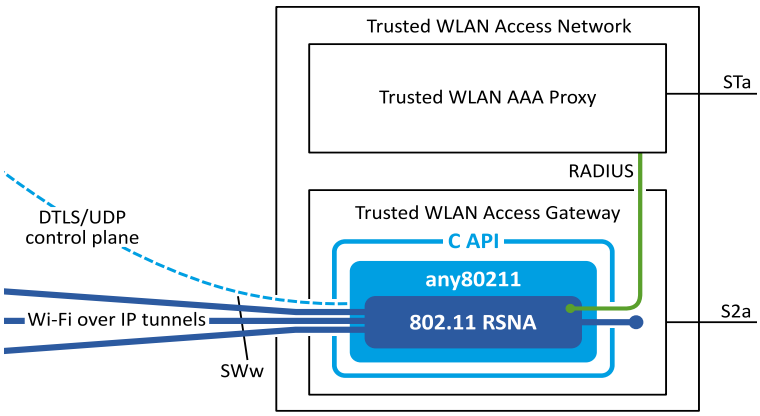
RELATED SOLUTIONS

- Secure mobile offload with SDWN App MOBILE

OVERVIEW

The SDWN architecture partitions the IEEE 802.11 stack into three parts: a low-level radio portion that runs on the access point and handles the real-time aspects of the Wi-Fi protocol, a high-level portion that performs the security processing and a Controller that connects the previous two through an IEEE 802.11 over UDP/IP data plane tunnel.

The high-performance Gateway Software link library allows termination of IEEE 802.11 over UDP/IP tunnels on a massive scale. It can be integrated in service router platforms and Wi-Fi gateways, ensuring compatibility with all access points incorporating Anyfi.net software.



The Gateway Software and its place in a 3GPP Trusted WLAN Access Network: Authenticating WLAN UE using RADIUS towards the Trusted WLAN AAA Proxy (TWAP) and delivering Ethernet frames between WLAN UE and the Trusted WLAN Access Gateway (TWAG). RADIUS is used for AAA and change of authorization (CoA). All communication with the outside world goes through a C API.

UNTRUSTED ACCESS POINTS AS A TRUSTED ACCESS?

3GPP makes a clear distinction between trusted and untrusted WLAN access. Question is, can you really trust access points that may be under the physical control of an attacker? The SDWN architecture lets you answer that question in the negative, while still integrating into them into the network as a trusted non-3GPP access.

How is that possible? By extending the SWw interface (IEEE Std 802.11) over the backhaul and terminating it directly in the Trusted WLAN Access Gateway (TWAG) you remove the access point from the security equation: even an attacker with complete control over the access point can only get to the encrypted IEEE 802.11 frames (SWw) – which are also available on the air interface.

ANYFI GATEWAY SOFTWARE

DATASHEET

HIGH-PERFORMANCE LINK LIBRARY EDITION

C API – NORTHBOUND INTERFACES

- RADIUS *(RFC2865, RFC2866, RFC2868, RFC2869, RFC3579, RFC4849, RFC5176)*
- SDWN control plane *(DTLS/UDP/IP)*

C API – WESTBOUND INTERFACES

- IEEE 802.11 over UDP/IP *(3GPP SWw)*

C API – EASTBOUND INTERFACES

- Ethernet / Dynamic VLAN

C API – CONFIGURABILITY

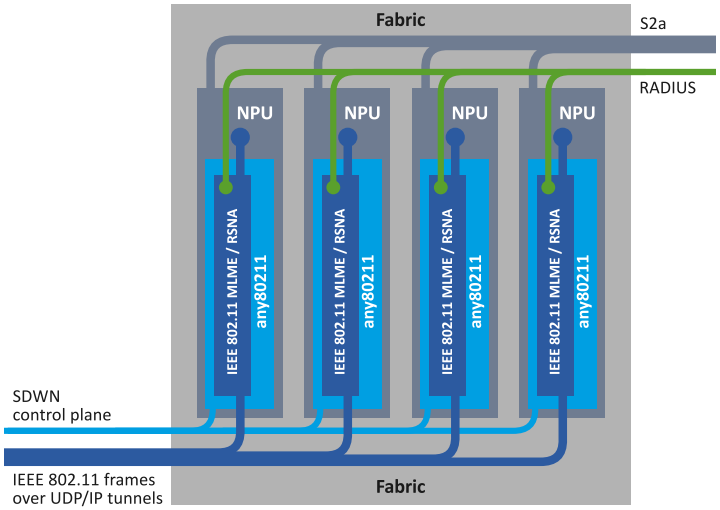
- IEEE 802.11 SSID
- IEEE 802.11 Auth Protocol *(WPA/RSN/FT)*
- IEEE 802.11 Auth Mode *(PSK/EAP)*
- IEEE 802.11 Encryption *(CCMP/TKIP)*
- IEEE 802.11 Preauthentication On/Off
- IEEE 802.11 Group Rekey Interval
- IEEE 802.11 Strict Rekey On/Off
- RADIUS authentication server
- RADIUS accounting server

KEY FEATURES

- EAP-SIM/AKA/AKA'/TLS/TTLS/PEAP etc.
- PMK key caching *(FT, PMKSA caching, OKC)*
- Traffic steering based on IMSI/MAC
- Hardware load balancing compatible

HARDWARE SUPPORT

- x86_64
- MIPS64



Internal architecture of a Wi-Fi gateway with IEEE 802.11 over UDP/IP tunnel termination software: Incoming IEEE 802.11 over UDP/IP tunnels are split up onto separate NPUs by a hardware load balancer and terminated in the link library ("any80211"). The resulting Ethernet frames are handed over to the surrounding process (TWAG) for further eastbound processing.

FUNCTIONALITY AND INTEGRATION

The high-performance Gateway Software link library is an ISO C implementation of the IEEE 802.11 MLME and RSNA, with integrated IEEE 802.1X authenticator. The library is entirely driven from the containing process, executing only when explicitly called on to handle an incoming IEEE 802.11 over UDP/IP packet, an outgoing Ethernet frame or the expiration of a timer. All communication with the outside world goes through a well-defined C API, ensuring that the library itself has no dependencies on third party or system libraries.

Integration in even the most arcane NPU platform is a breeze. Simply implement a small glue layer towards the library and let it handle all the rest. Packet data is passed in and out of the library as pointers, ensuring zero copy processing. The library is available in ISO C source code form, or as linkable object code compiled for x86_64 and MIPS64 target CPUs.

Anyfi Networks

Carrier Wi-Fi That Just Works