

EX1044

The Apple Wiki

Apple Push Notification Service

From The Apple Wiki

Introduced in iPhoneOS 3, **Apple Push Notification Service** ("APNs", also known as "Apple Push Service Protocol") allows devices to receive and display push notifications from an app, even when the app is not running. APNs allows the device to subscribe to "topics", and only notifications matching the subscribed topics will be delivered. In addition to receiving, the protocol can also be used to send messages to other devices. This mechanism is not only used by push notifications, but also by other real-time interactions such as iMessage and HomeKit.

APNs communicates over TLS on TCP port 5223 (although it can fall back to port 443). It connects to a subdomain of `push.apple.com`, either dynamically determined or static, depending on the platform.

A device identifies itself to APNs by proving that it controls a certificate obtained from Albert. Initially, this was done using TCP client certificates, but this allowed fingerprinting.^[1] In response, Apple introduced an upgraded protocol called `apns-security-v3`, which must be negotiated over ALPN.

The binary protocol used in APNs has evolved over time. The initial versions used a proprietary binary protocol in a simple type-length-value encoding. Each message was preceded by a "command". The initial version used until iOS 4 used commands `00` to `06`. In iOS 5, the protocol was upgraded to use the new commands `07` and above.^[2] Some commands have been added in iOS versions since then.^[3]

In iOS 10, Apple introduced `apns-pack-v1`, which is a packed version of the existing protocol designed to be byte-efficient. However, it is not necessary to use this encoding, as several official platforms still use the old protocol. The new protocol is also negotiated over ALPN, and it is possible to force iOS to downgrade to the old protocol.^[4]

Protocol details

References

1. Push Away Your Privacy: Precise User Tracking Based on TLS Client Certificate Authentication (https://tma.ifip.org/wordpress/wp-content/uploads/2017/06/tma2017_paper2.pdf)
2. Apple Push Service Protocol: iOS 5 (<https://github.com/meeeee/pushproxy/blob/master/doc/apple-push-protocol-ios5-lion.md>)

3. [APNs Dissector: APNs Command Info \(https://gitlab.com/nicolas17/apns-dissector/-/blob/master/apns-command-info.yml\)](https://gitlab.com/nicolas17/apns-dissector/-/blob/master/apns-command-info.yml)
4. [APNs Dissector \(https://gitlab.com/nicolas17/apns-dissector/\)](https://gitlab.com/nicolas17/apns-dissector/)

[v · t · e](https://theapplewiki.com/index.php?title=Template:Navbox_Protocols&action=edit) (https://theapplewiki.com/index.php?title=Template:Navbox_Protocols&action=edit)

Protocols

Boot	iBoot (Bootrom · LLB · iBSS (iBootStage1) · iBEC (iBootStage2) · iBoot) · Normal Mode · Recovery Mode (Protocols) · Restore Mode · DFU Mode
USB	usbmux · lockdownd · WTF · Factory Data Restore · USB Target Disk Mode · Serial Wire Debug
Baseband	Bootrom · Bootloader · Firmware · Commands
OS Services	AFC
Online Services	Albert · GSA · APNs · IDS · CloudKit · MMCS · Siri



Retrieved from "https://theapplewiki.com/index.php?title=Apple_Push_Notification_Service&oldid=219969"