Cracking Open What Makes Apple's Low-Latency WiFi So Fast

A Deep Dive into Tracing the Network Stack on macOS and iOS

Henri Jäger

whoami

Student @ Hasso Plattner Institute

Mobile and Wireless Security

HPI Hasso Plattner Institut

Digital Engineering · Universität Potsdam

[12]

Researcher @ OpenKRITIS

EU / German Cyber Security Regulations

OpenKRITIS NIS2 Europa Betreiber Security School

KRITIS – auf den zweiten Blick

OpenKRITIS ist eine unabhängige Plattform für den Schutz Kritischer Infrastrukturen. Wir unterstützen Betreiber und Prüfer in der KRITIS und NIS2-Regulierung: Klare Strukturen zur Umsetzung von Cybersecurity, Governance und Prüfungen.

KRITIS und NIS2

[D]

Kritische Infrastrukturen

[1] [2] [3] [4]

Sidecar Display

Previous research on Continuity Camera and Sidecar Display has been conducted by Inga Dischinger [A] and Jan Röper [B]

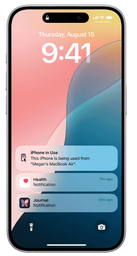
Universal Control

[5] [6] [7]

Continuity Camera

[9] [10]

iPhone Mirroring



Continuity features and requirements for Apple devices

Continuity features make it seamless to move between your Mac, iPhone, iPad, Apple Watch, Apple TV, and Apple Vision Pro devices that meet the system requirements.

AirDrop

AirPlay to Mac

Apple Pay

Auto Unlock

Continuity Camera: Use iPhone as a webcam for Mac

Continuity Camera: Use iPhone or iPad as a webcam for Apple TV

Continuity Camera: Use iPhone or iPad to take photos or scan documents on Mac

Continuity Sketch and Continuity Markup

Handoff

Instant Hotspot

iPhone Cellular Calls

iPhone Mirroring

iPhone widgets on Mac

Mac Virtual Display

Mirror My View

Sidecar

Text Message Forwarding

Universal Clipboard

Universal Control

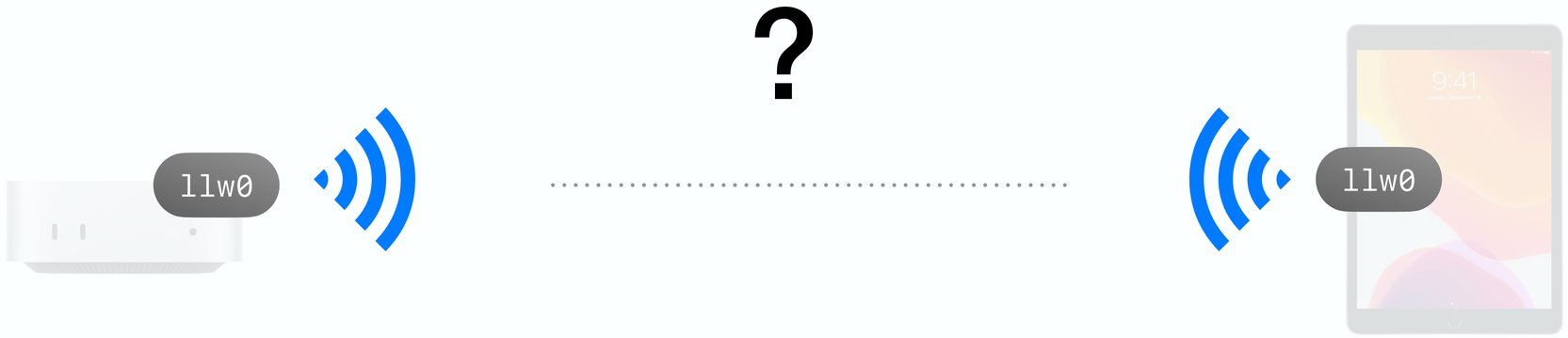
[C]

Mostly Video Data

Real-Time Constraints

Low-Latency WiFi 🪄


llw0
9:41
Tuesday, September 10
llw0



How is this interface opened?

Are other devices LLW-compatible?

What makes LLW *low-latency* WiFi?

Logging

Kernel Traces

XPC Communication

Backtraces

Packet Captures

```
en0, awdl0, llw0, BLE, ...
```

Logging

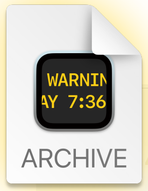
Kernel Traces

XPC Communication

Backtraces

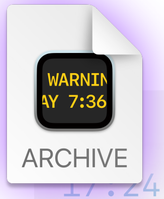
Missing Solution

to correlate log information from different log sources in a timely manner




```
17:24:16.704 SidecarDisplayAgent        === Sideca
17:24:16.772 rapportd     Added policy: order = 9 re
17:24:16.792 kernel.development         SK[1]: channe
17:24:17.542 avconferenced              VCMediaStream
17:24:18.565 kernel.development         SK[7]: ch_eve
17:24:18.566 airportd     [corewifi] @[13190.661012]
17:24:22.688 SidecarRelay nw_channel_create_with_nex
17:24:24.563 mDNSResponder SysEventCallBack -- event
17:24:24.563 configd      Process interface link up:
17:24:24.566 nsattributedstringagent    SLSTransacti
```

```
4:17.127 SidecarRelay === IDS F090DC4A:remote:/
17:24:17.128 kernel       wlan0:com.apple.p2p: AWDLS
17:24:17.130 rapportd     48: SendEventID 'com.apple
17:24:17.133 runningboardd              _checkForSusp
17:24:28.103 wifip2pd     XPCSession[avconferenced 1
17:24:19.931 +0200        avconferenced [C96 IPv6#5c
17:24:20.588 kernel       rt_lookup_common:3376 (::,
17:24:23.170 kernel       wlan0:com.apple.p2p: IO802
17:24:25.972 kernel       cacheVerifiedACM <- reset
17:24:27.973 kernel AppleBiometricServices::message
```




```
17:24:16.704 SidecarDisplayAgent       === Sidecar (
17:24:16.772 rapportd     Added policy: order = 9 re
17:24:17.128 kernel       wlan0:com.apple.p2p: AWDLS
17:24:16.792 kernel.development        SK[1]: channe
17:24:17.130 rapportd     48: SendEventID 'com.apple
17:24:17.133 runningboardd             _checkForSusp
17:24:18.103 wifip2pd     XPCSession[avconferenced 1
17:24:17.542 avconferenced             VCMediaStream
17:24:18.565 kernel.development        SK[7]: ch_eve
17:24:19.931 +0200        avconferenced [C96 IPv6#5c
17:24:18.566 airportd     [corewifi] @[13190.661012]
17:24:20.588 kernel       rt_lookup_common:3376 (::,
17:24:23.170 kernel       wlan0:com.apple.p2p: IO802
17:24:22.688 SidecarRelay nw_channel_create_with_nex
17:24:25.972 kernel       cacheVerifiedACM <- reset
17:24:24.563 mDNSResponder SysEventCallBack -- event
17:24:24.563 configd      Process interface link
```

Log Aggregator

Network Stack on macOS and iOS

Low-Latency in LLW

Building a Log Aggregator

Challenges

Log Aggregation & Collection

Availability of forensic sources (iOS)

Clock offsets

Collection on multiple devices

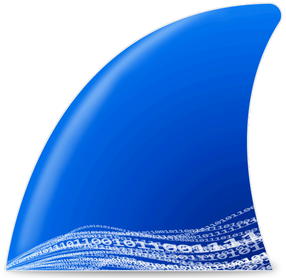
Aggregation of varying file formats

Noise filtering

Console

dtrace

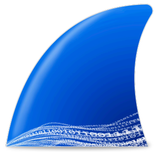
ktrace



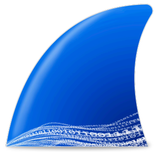
Wireshark

cctool

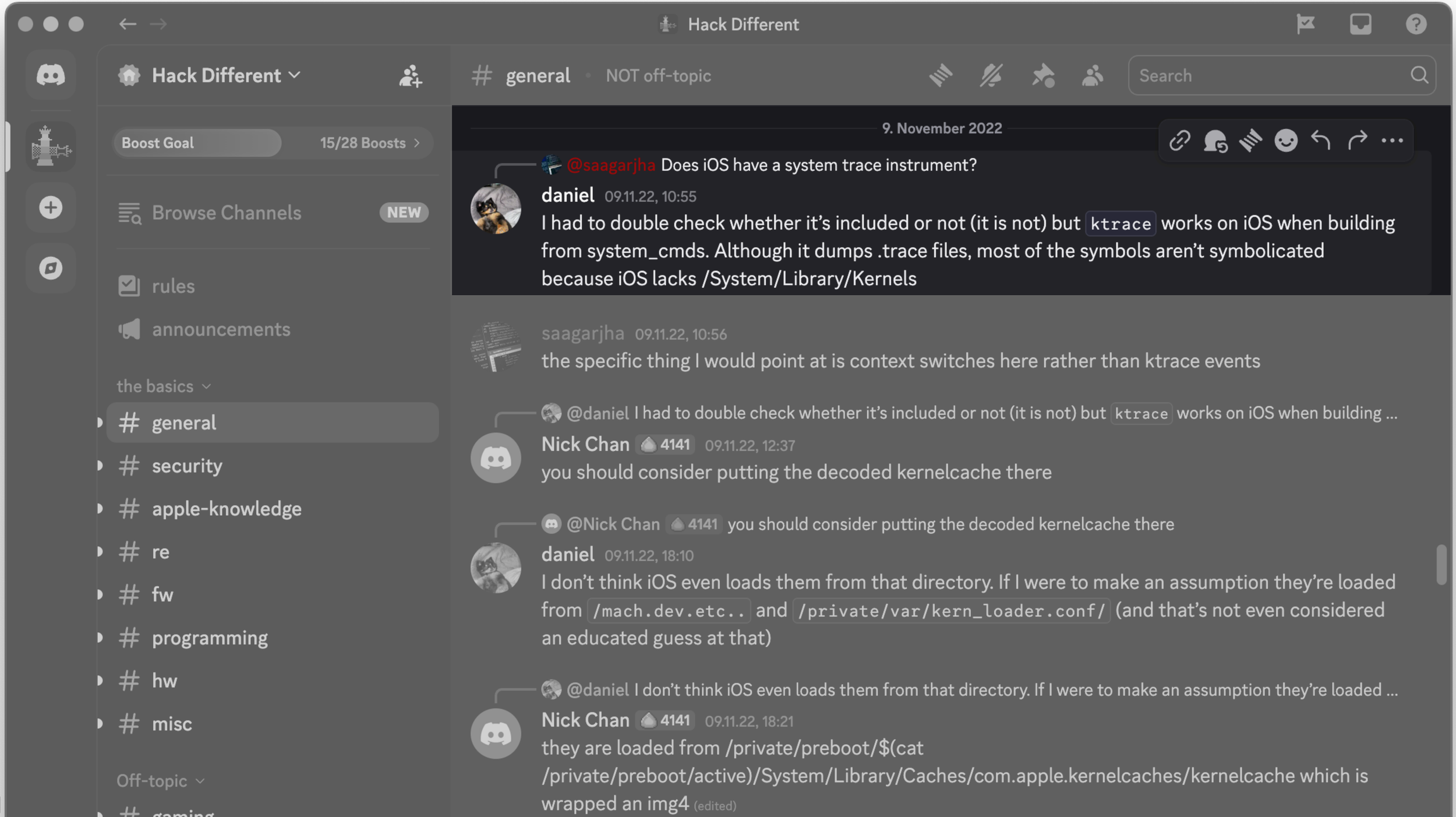
PacketLogger

						
macOS	✅	✅	✅	✅	✅	✅
iOS	✅ `log`	✅ `tcpdump*`	✅	🤔	🤔	🤔

* Jailbreak required — our setup includes an iPad (7th generation)

						
macOS	✅	✅	✅	✅	✅	✅
iOS	✅ `log`	✅ `tcpdump*`	✅	❌	✅ from source*	✅ reimplementation*

* Jailbreak required — our setup includes an iPad (7th generation)


Hack Different
Hack Different
Boost Goal
15/28 Boosts
Browse Channels
NEW
rules
announcements
the basics
general
security
apple-knowledge
re
fw
programming
hw
misc
Off-topic
general
NOT off-topic
Search
9. November 2022
@saagarjha Does iOS have a system trace instrument?
daniel 09.11.22, 10:55
I had to double check whether it's included or not (it is not) but ktrace works on iOS when building from system_cmds. Although it dumps .trace files, most of the symbols aren't symbolicated because iOS lacks /System/Library/Kernels
saagarjha 09.11.22, 10:56
the specific thing I would point at is context switches here rather than ktrace events
@daniel I had to double check whether it's included or not (it is not) but ktrace works on iOS when building ...
Nick Chan 4141 09.11.22, 12:37
you should consider putting the decoded kernelcache there
@Nick Chan 4141 you should consider putting the decoded kernelcache there
daniel 09.11.22, 18:10
I don't think iOS even loads them from that directory. If I were to make an assumption they're loaded from /mach.dev.etc.. and /private/var/kern_loader.conf/ (and that's not even considered an educated guess at that)
@daniel I don't think iOS even loads them from that directory. If I were to make an assumption they're loaded ...
Nick Chan 4141 09.11.22, 18:21
they are loaded from /private/preboot/$(cat /private/preboot/active)/System/Library/Caches/com.apple.kernelcaches/kernelcache which is wrapped an img4 (edited)

Hack Different

Hack Different

Boost Goal 15/28 Boosts

Browse Channels NEW

rules

announcements

the basics

general

security

apple-knowledge

re

fw

programming

hw

misc

Off-topic

general • NOT off-topic

Search

9. November 2022

@saagarjha Does iOS have a system trace instrument?

daniel 09.11.22, 10:55

I had to double check whether it's included or not (it is not) but `ktrace` works on iOS when building from system_cmds. Although it dumps .trace files, most of the symbols aren't symbolicated because iOS lacks /System/Library/Kernels

system_cmds

rather than ktrace events

not) but `ktrace` works on iOS when building ...

you should consider putting the decoded kernelcache there

@Nick Chan 4141 you should consider putting the decoded kernelcache there

daniel 09.11.22, 18:10

I don't think iOS even loads them from that directory. If I were to make an assumption they're loaded from `/mach.dev.etc..` and `/private/var/kern_loader.conf/` (and that's not even considered an educated guess at that)

@daniel I don't think iOS even loads them from that directory. If I were to make an assumption they're loaded ...

Nick Chan 4141 09.11.22, 18:21

they are loaded from /private/preboot/$(cat /private/preboot/active)/System/Library/Caches/com.apple.kernelcaches/kernelcache which is wrapped an img4 (edited)

Platform Solutions Resources Open Source Enterprise Pricing

Sign in Sign up

apple-oss-distributions / system_cmds Public

Notifications Fork 8 Star 39

Code Pull requests Security Insights

main Go to file Code

AppleOSSDistributions system_cmds-10... e0c267e · 2 months ago 30 Commits

GCoreFrameworkTests	system_cmds-1039	2 months ago
ac	system_cmds-970.0.4	2 years ago
accton	system_cmds-970.0.4	2 years ago
arch	system_cmds-1012	last year
at	system_cmds-1012	last year
atrun	system_cmds-1012	last year
chkpasswd	system_cmds-970.0.4	2 years ago

About

opensource.apple.com/releases

Activity

Custom properties

39 stars

4 watching

8 forks

Report repository

Releases

72 tags

getty	system_cmds-970.0.4	2 years ago
hostinfo	system_cmds-970.0.4	2 years ago
iosim	system_cmds-970.0.4	2 years ago
iostat	system_cmds-970.0.4	2 years ago
kpgo	system_cmds-970.0.4	2 years ago
latency	system_cmds-970.0.4	2 years ago
login	system_cmds-1012	last year
lskq	system_cmds-979.100.8	last year

???

Platform Solutions Resources Open Source Enterprise Pricing

Sign in Sign up

apple-oss-distributions / system_cmds Public

Notifications Fork 8 Star 39

Code Pull requests Security Insights

Releases Tags

system_cmds...

559f661

Compare

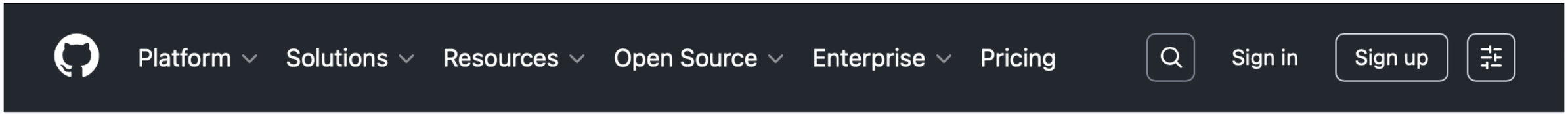
system_cmds-918.100.3

AppleOSSDistributions tagged this Apr 26, 2022

```
Imported from system_cmds-918.100.3.tar.gz
```

Assets 2

Source code (zip)	Apr 26, 2022
Source code (tar.gz)	Apr 26, 2022



apple-oss-distributions / system_cmds Public

Notifications | Fork 8 | Star 39

Code | Pull requests | Security | Insights

Files

559f661

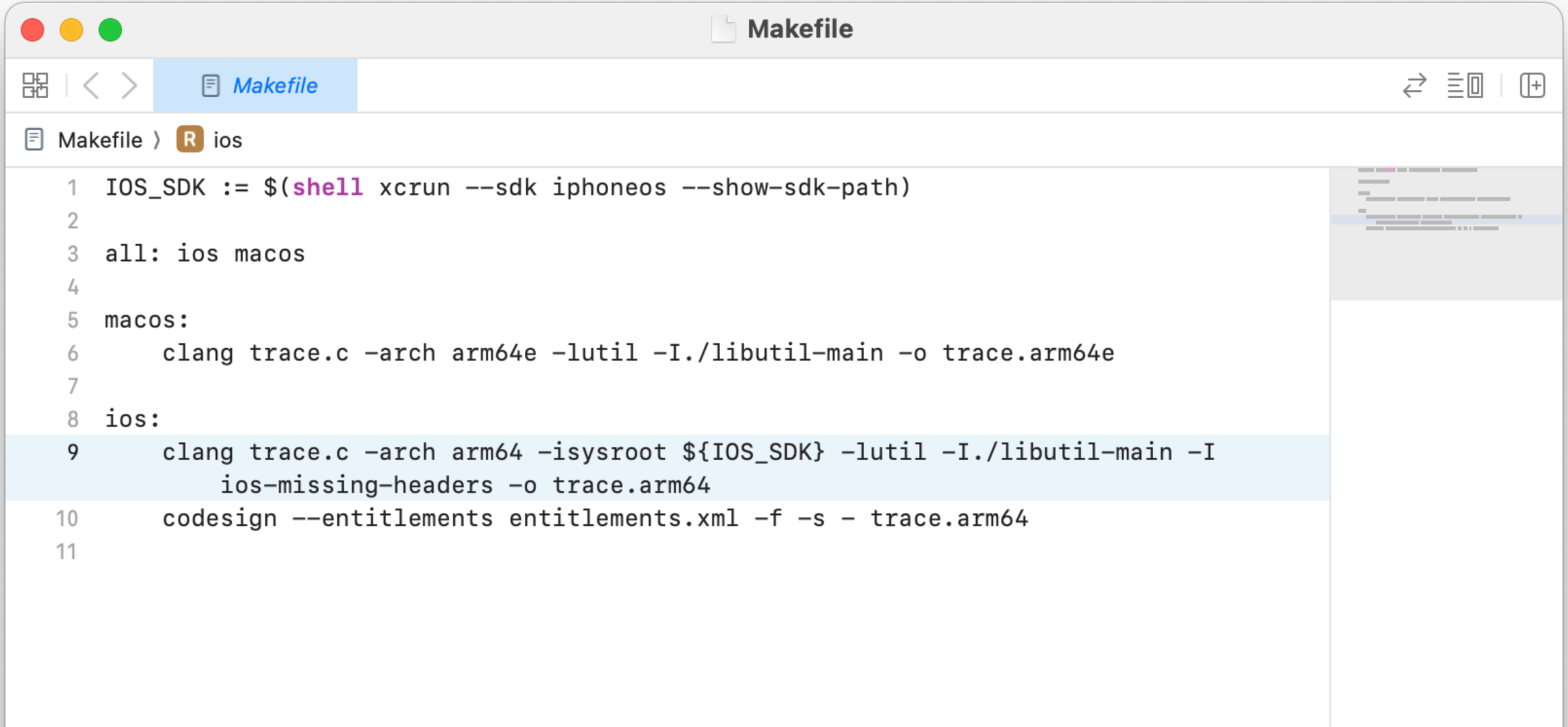
Go to file

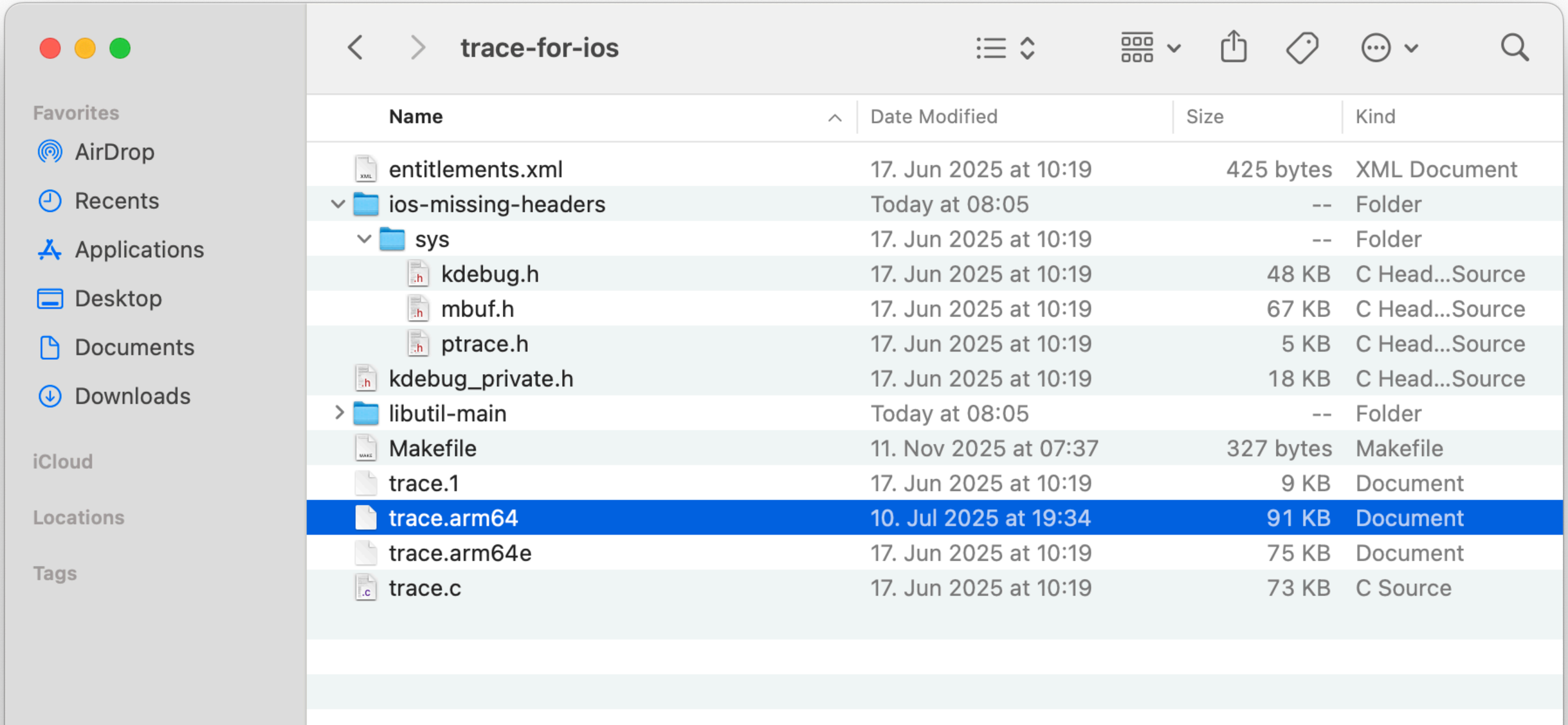
- ac.tproj
- accton.tproj
- arch.tproj
- at.tproj
- atrun.tproj
- chkpasswd.tproj

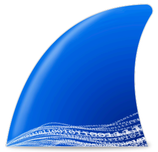
system_cmds / trace.tproj /

AppleOSSDistributions system_cmds-916 — 16245aa · 3 years ago — History

Name	Last commit message	Last commit date
..		
trace.1	system_cmds-916	3 years ago
trace.c	system_cmds-854.11.2	4 years ago


Makefile
Makefile
Makefile ⟩ R ios
1 IOS_SDK := $(shell xcrun --sdk iphoneos --show-sdk-path)
2
3 all: ios macos
4
5 macos:
6 clang trace.c -arch arm64e -lutil -I./libutil-main -o trace.arm64e
7
8 ios:
9 clang trace.c -arch arm64 -isysroot ${IOS_SDK} -lutil -I./libutil-main -I
ios-missing-headers -o trace.arm64
10 codesign --entitlements entitlements.xml -f -s - trace.arm64
11


trace-for-ios
Favorites
AirDrop
Recents
Applications
Desktop
Documents
Downloads
iCloud
Locations
Tags
Name
Date Modified
Size
Kind
entitlements.xml 17. Jun 2025 at 10:19 425 bytes XML Document
ios-missing-headers Today at 08:05 -- Folder
sys 17. Jun 2025 at 10:19 -- Folder
kdebug.h 17. Jun 2025 at 10:19 48 KB C Head...Source
mbuf.h 17. Jun 2025 at 10:19 67 KB C Head...Source
ptrace.h 17. Jun 2025 at 10:19 5 KB C Head...Source
kdebug_private.h 17. Jun 2025 at 10:19 18 KB C Head...Source
libutil-main Today at 08:05 -- Folder
Makefile 11. Nov 2025 at 07:37 327 bytes Makefile
trace.1 17. Jun 2025 at 10:19 9 KB Document
trace.arm64 10. Jul 2025 at 19:34 91 KB Document
trace.arm64e 17. Jun 2025 at 10:19 75 KB Document
trace.c 17. Jun 2025 at 10:19 73 KB C Source



macOS	✅	✅	✅	✅	✅	✅
iOS	✅ `log`	✅ `tcpdump*`	✅	❌	✅ from source*	✅ reimplementation*

* Jailbreak required — our setup includes an iPad (7th generation)

Challenges

Log Aggregation & Collection

Availability of forensic sources (iOS)

Clock offsets

Collection on multiple devices

Aggregation of varying file formats

Noise filtering

Logging

Kernel Traces

XPC Communication

Backtraces

Packet Captures

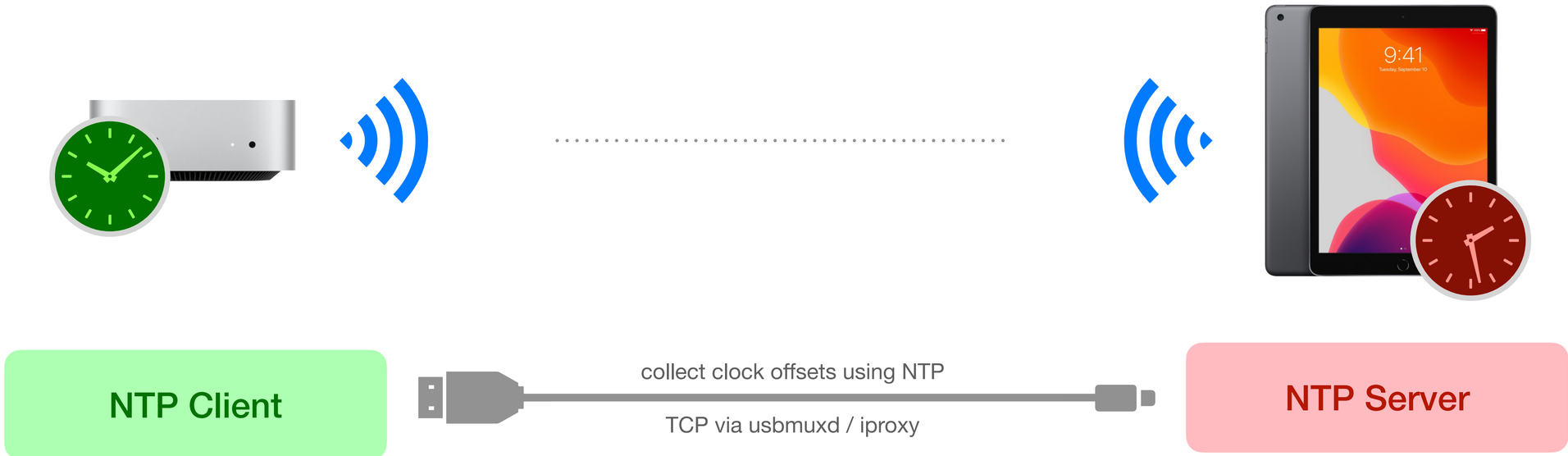
`en0, awdl0, llw0, BLE, ...`

Logging

Kernel Traces

XPC Communication

Backtraces


9:41
NTP Client
collect clock offsets using NTP
TCP via usbmuxd / iproxy
NTP Server

Challenges

Log Aggregation & Collection

Availability of forensic sources (iOS)

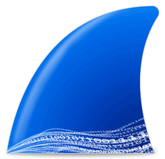
Clock offsets

Collection on multiple devices

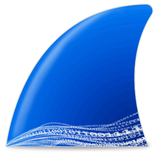
Aggregation of varying file formats

Noise filtering

Collect Logs



Aggregate Logs



macOS	✅	✅	✅	✅	✅	✅
iOS	✅ `log`	✅ `tcpdump*`	✅	❌	✅ from source*	✅ reimplementation*

* Jailbreak required — our setup includes an iPad (7th generation)

log-acquisition.sh

User Interface

`log-acquisition.sh --format=pcap`

log-acquisition-idevice-lib.sh

Remote Device Management

`get_latest_dir_on_iPad(), ...`

log-acquisition-iOS.sh

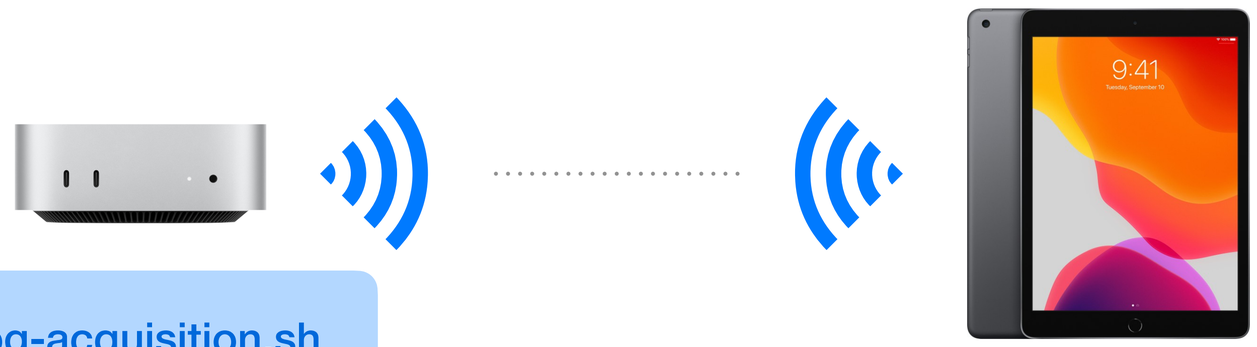
log-idevice-ssh-interface.sh

SSH communication

`start_iproxy(), send_to_iPad(), ...`

listener-iOS.sh

ssh tunnel



log-acquisition.sh

log-acquisition-idevice-lib.sh

log-idevice-ssh-interface.sh

log-acquisition-iOS.sh

listener-iOS.sh

ssh tunnel

Process Management

`start_pre_session_commands(), ...`

Command Injection

`Relay remote commands to upper layer`

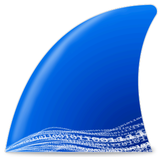
log-acquisition.sh

log-acquisition-iOS.sh

log-acquisition-idevice-lib.sh

log-idevice-ssh-interface.sh

listener-iOS.sh



tunnel

cc tool

d trace

k trace

...

1. Connect iPad to Mac
2. Script starts captures on iPad and Mac (`tcpdump`, `trace` | `tshark`, `dtrace`, `ktrace`, `PacketLogger`)
3. Start Sidecar Display session

   …
4. End Sidecar Display session
5. Script collects log information on iPad and Mac (`cctool` | `cctool`, `log`)
6. Script transfers captures to Mac
7. Run log aggregation

Challenges

Log Aggregation & Collection

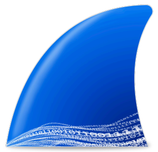
Availability of forensic sources (iOS)

Clock offsets

Collection on multiple devices

Aggregation of varying file formats

Noise filtering



macOS	✅	✅	✅	✅	✅	✅
iOS	✅ `log`	✅ `tcpdump*`	✅	❌	✅ from source*	✅ reimplementation*
File format	`.json`	`.pcapng` `.pcap`	`.pklg`	`custom`	`.json`	`.txt` `.pcapng`

Jailbreak required — our setup includes an iPad (7th generation)

ktrace output

Packet Captures

Log Archive

Text Files &
Custom Output

ktrace parser

pcapng parser

logarchive parser

dtrace parser

txt parser

Parse Input Files into Business Logic

Filter Pre-Recorded Noise

Apply Static Filter Criteria

Resolve Logs to
User / Kernel-Space Functions

Write .pcapng File
with `python-pcapng`

Log to
macOS' Unified Logging System

Challenges

Log Aggregation & Collection

Availability of forensic sources (iOS)

Clock offsets

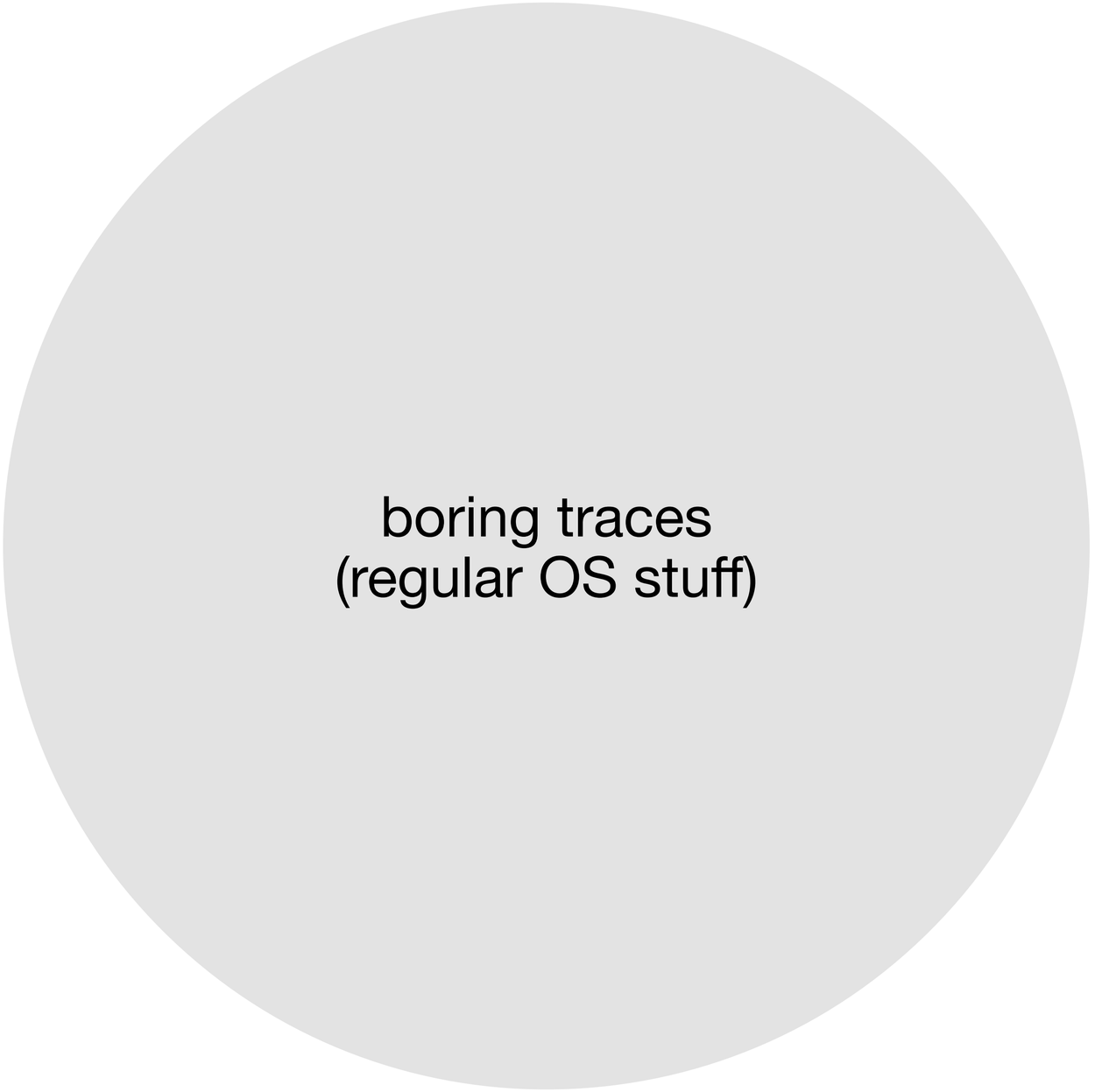
Collection on multiple devices

Aggregation of varying file formats

Noise filtering

boring traces
(regular OS stuff)

Record boring traces

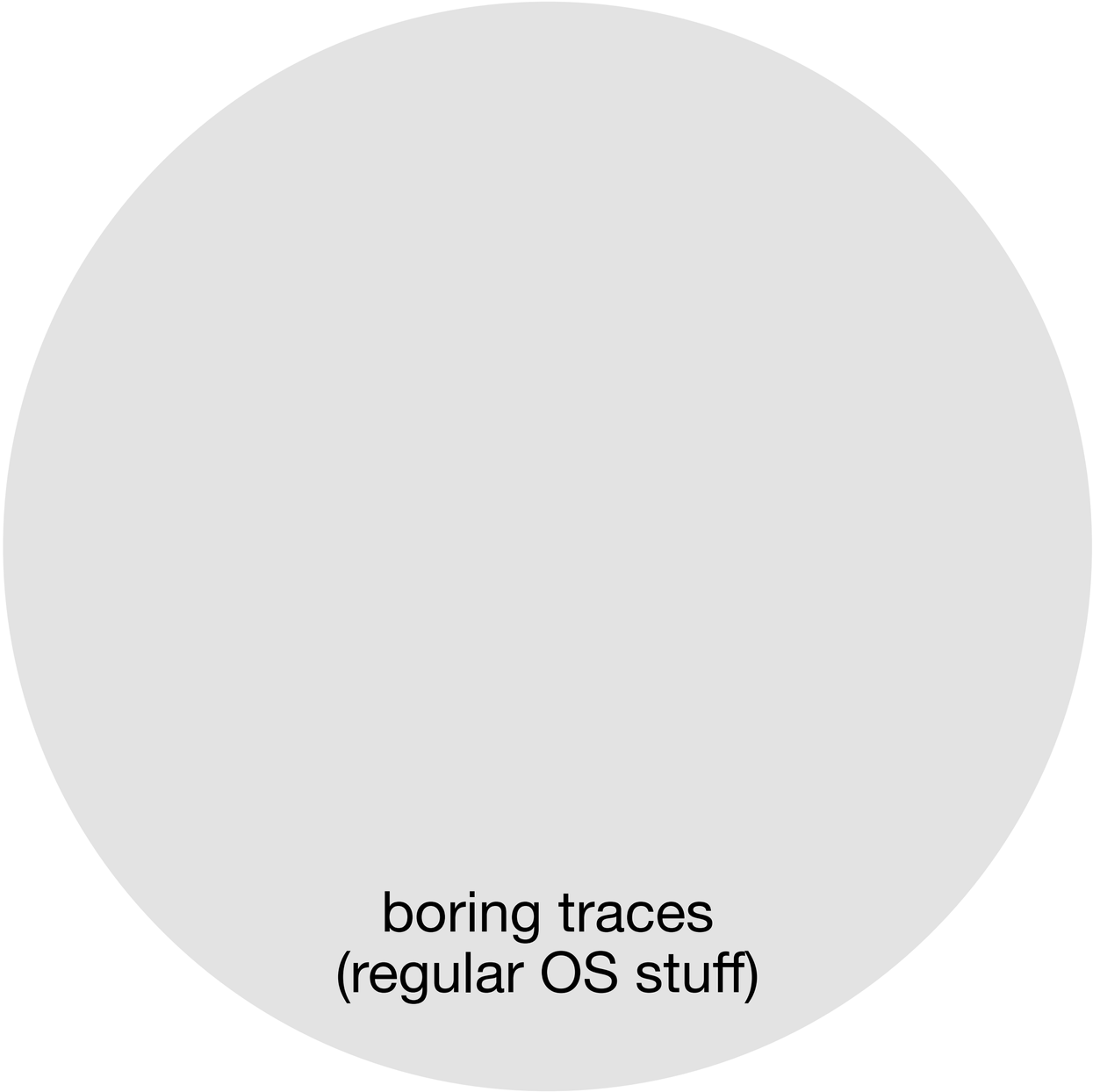


Record boring traces

Noise Reference Data

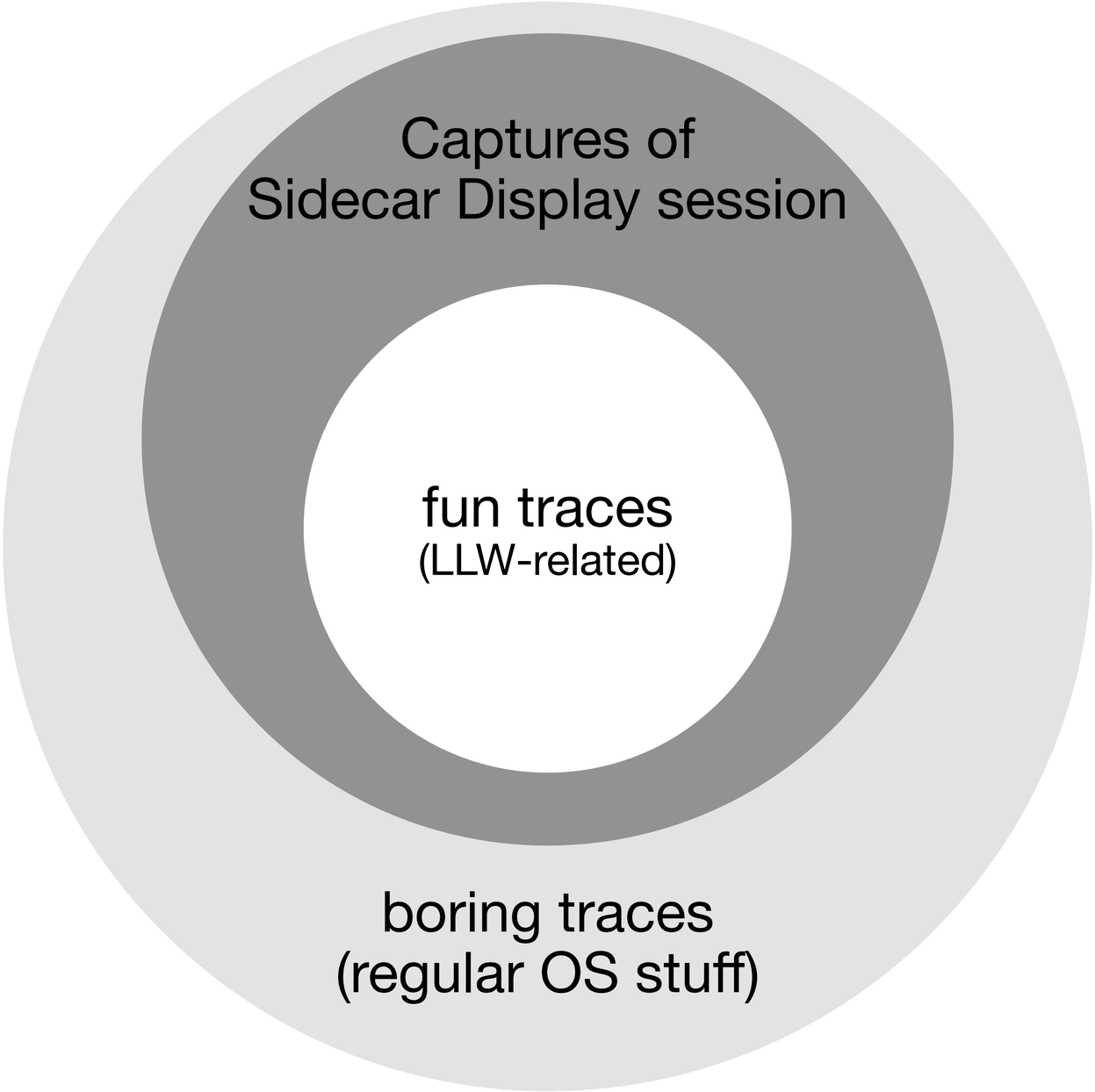
boring traces
(regular OS stuff)

Record boring traces



Record boring traces

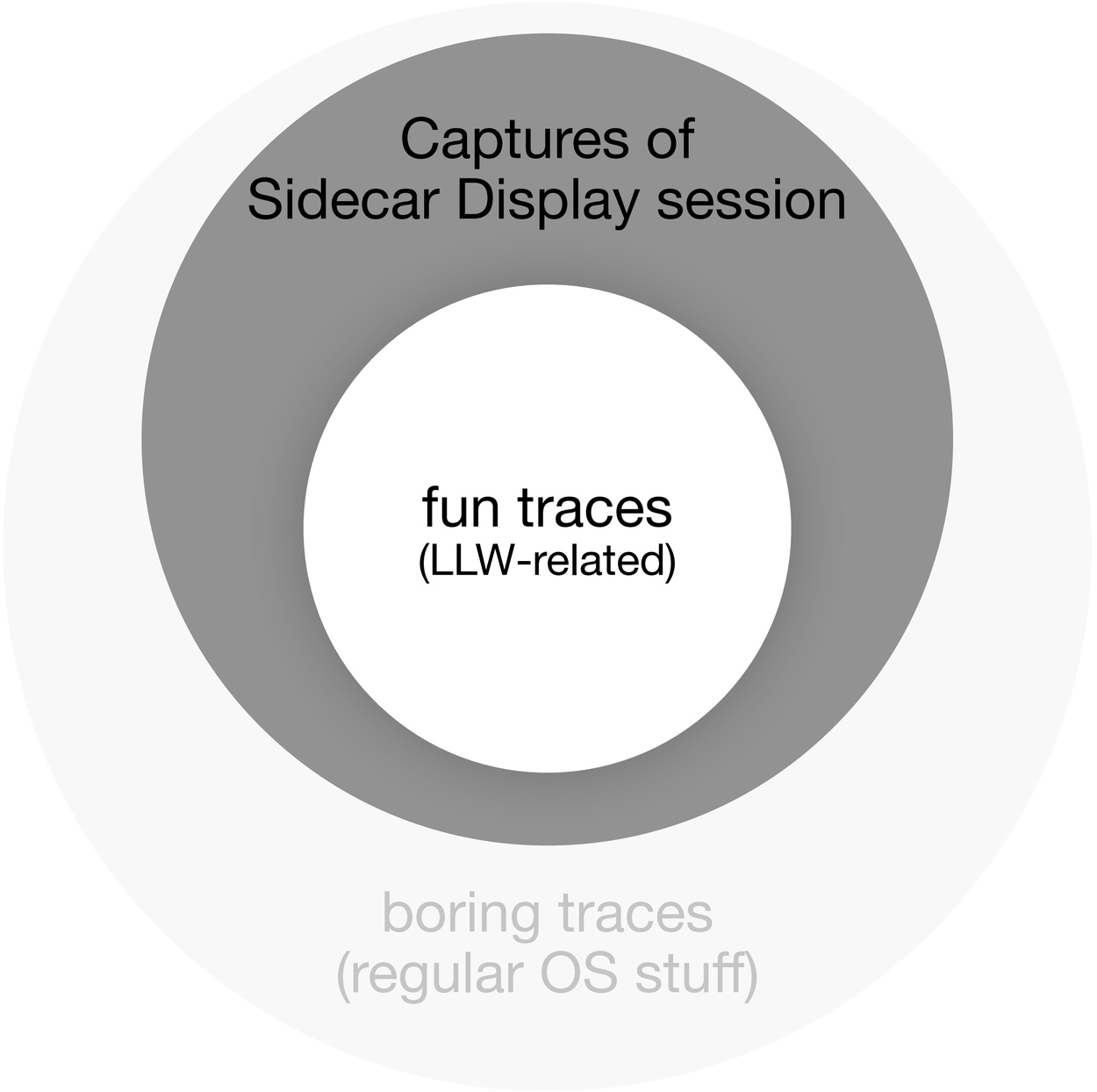
Record Sidecar Display captures

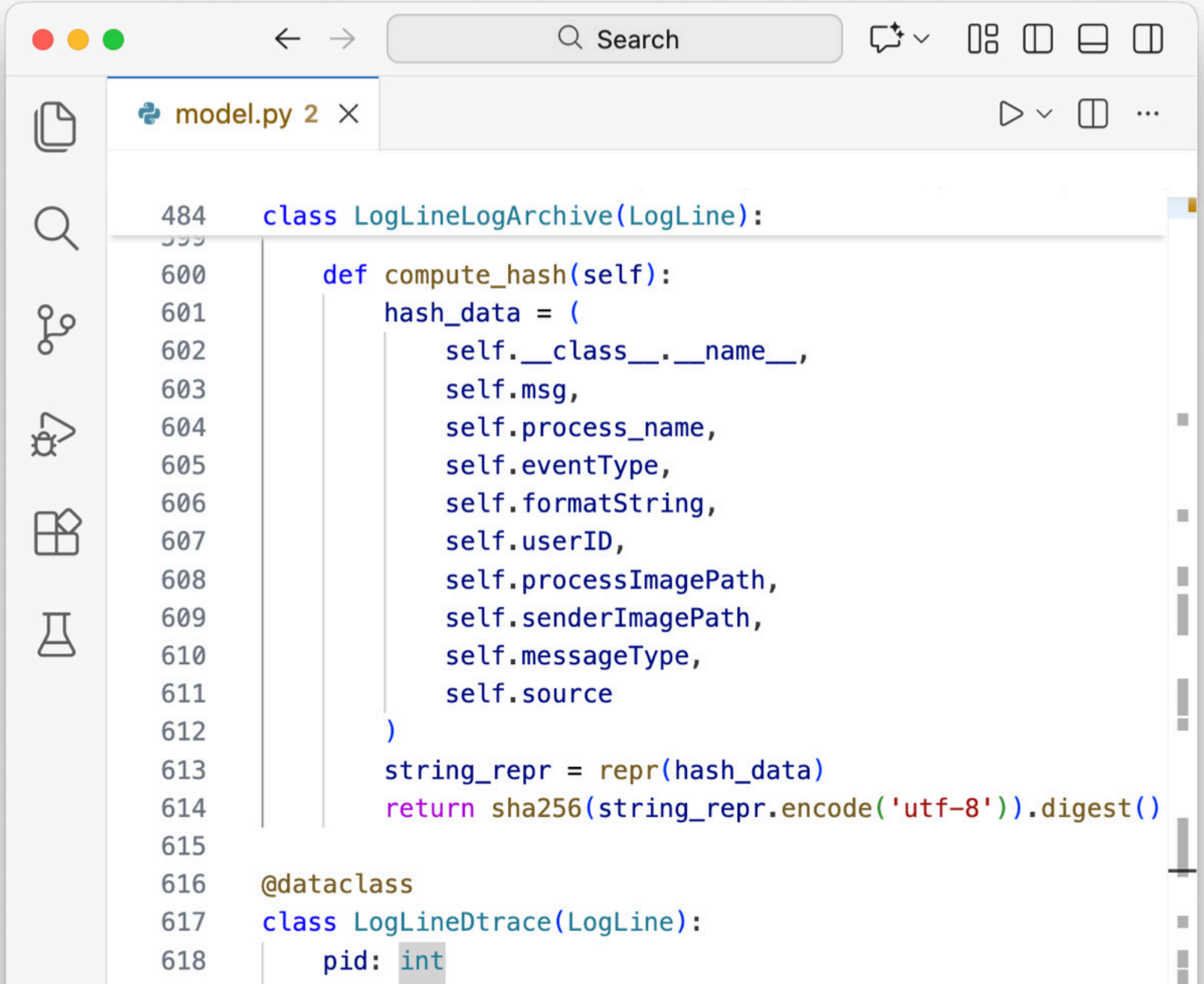


Record boring traces

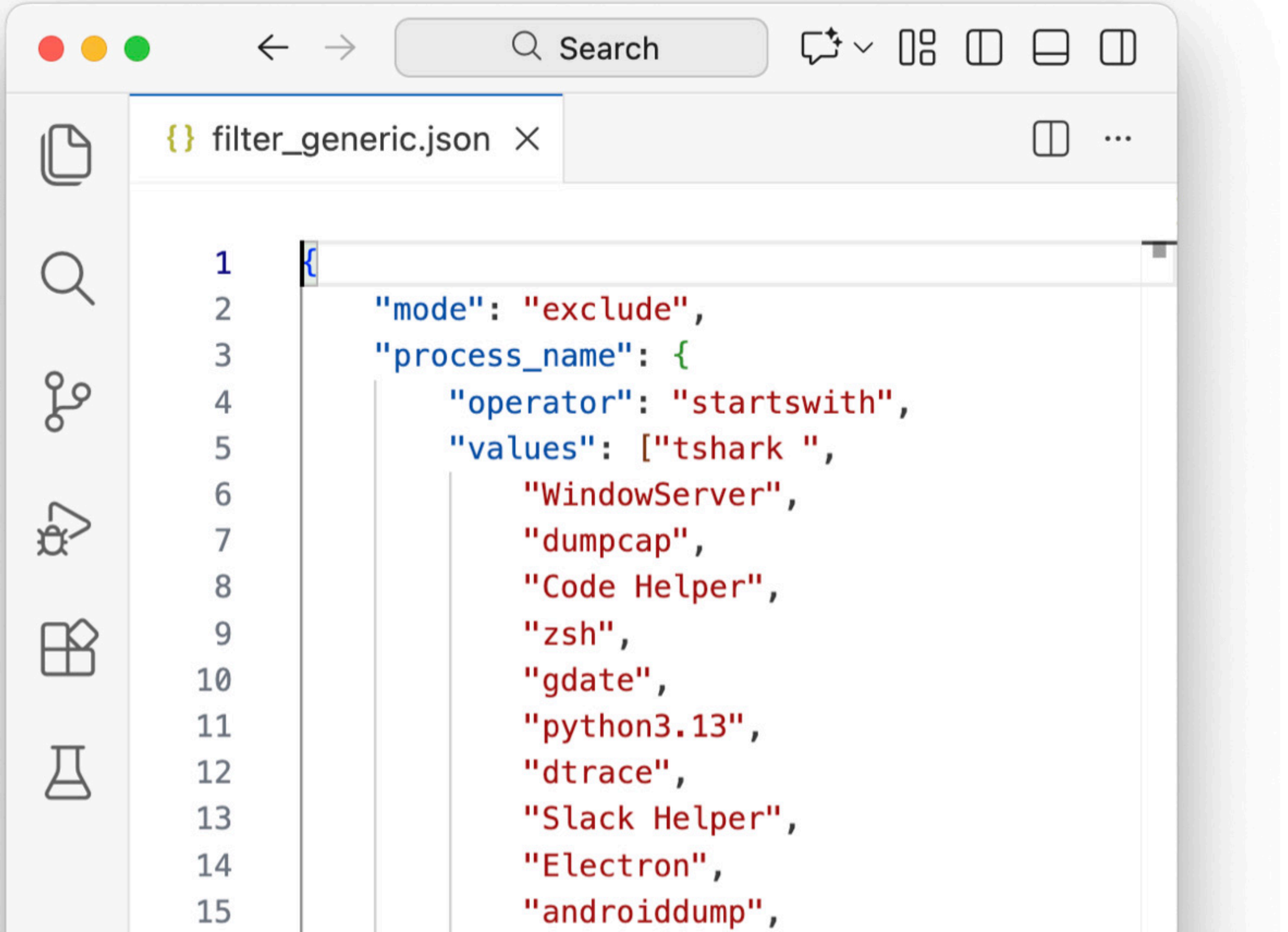
Record Sidecar Display captures

Keep the interesting ones




Search
model.py 2
484 class LogLineLogArchive(LogLine):
600 def compute_hash(self):
601 hash_data = (
602 self.__class__.__name__,
603 self.msg,
604 self.process_name,
605 self.eventType,
606 self.formatString,
607 self.userID,
608 self.processImagePath,
609 self.senderImagePath,
610 self.messageType,
611 self.source
612)
613 string_repr = repr(hash_data)
614 return sha256(string_repr.encode('utf-8')).digest()
615
616 @dataclass
617 class LogLineDtrace(LogLine):
618 pid: int

Static Filters



Challenges

Log Aggregation & Collection

Availability of forensic sources (iOS)

Clock offsets

Collection on multiple devices

Aggregation of varying file formats

Noise filtering

Backtrace Reconstruction

Log Aggregator TraceBlender

Multi-Device Support

k trace Support on iOS

cc tool Support on iOS

Multi-Device Log Aggregation & Collection

.pcap .json .pcapng

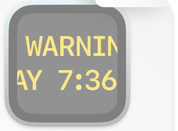
Support for 6+ Input Formats

custom output .pklg .txt

Clock Offset Correction

Log Collection Toolkit

Noise Filtering



Support for logarchive Output

Support for pcapng Output

Extensible to More Tracing Tools

Log Aggregator

Network Stack on macOS and iOS

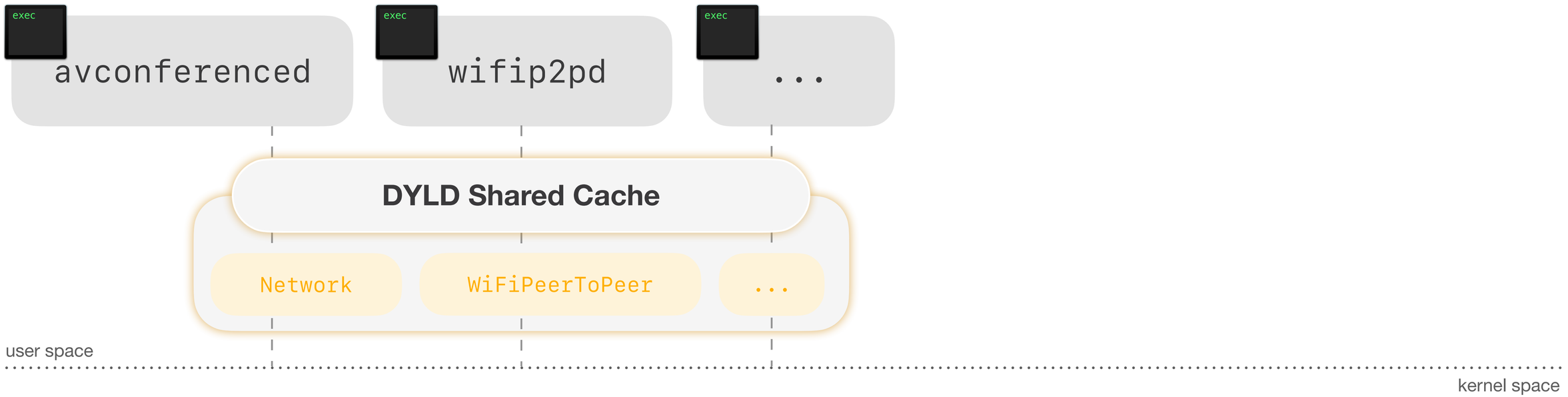
Low-Latency in LLW

Network Stack on macOS and iOS

System Components

Interface Lifecycle Management

Tracing the Network Stack on macOS and iOS



kernel

IOSkywalkFamily

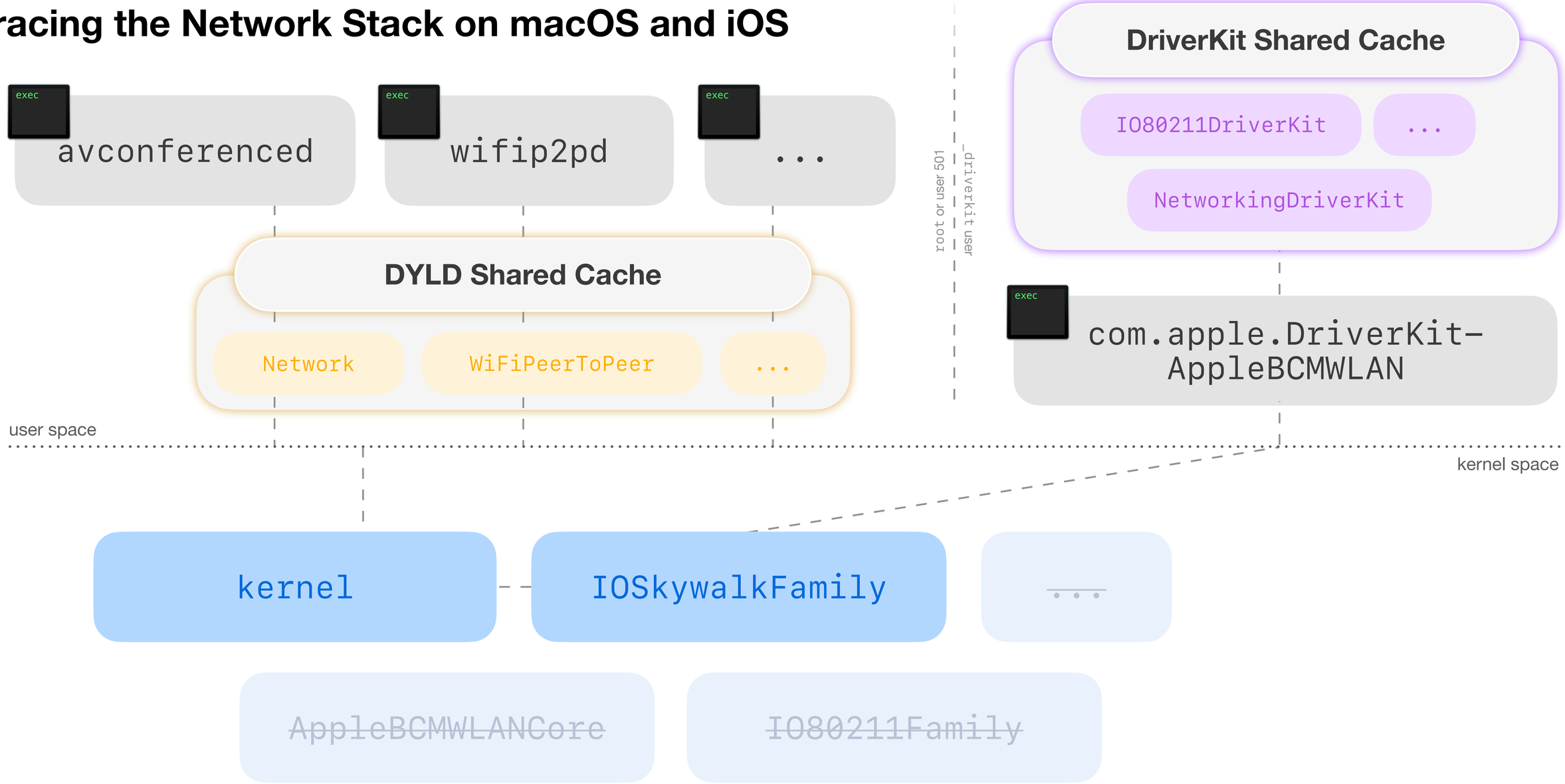
...

AppleBCMWLANCore

IO80211Family

* User space processes (left-hand side) were identified by Jan Röper [A] and Inga Dischinger [B]

Tracing the Network Stack on macOS and iOS



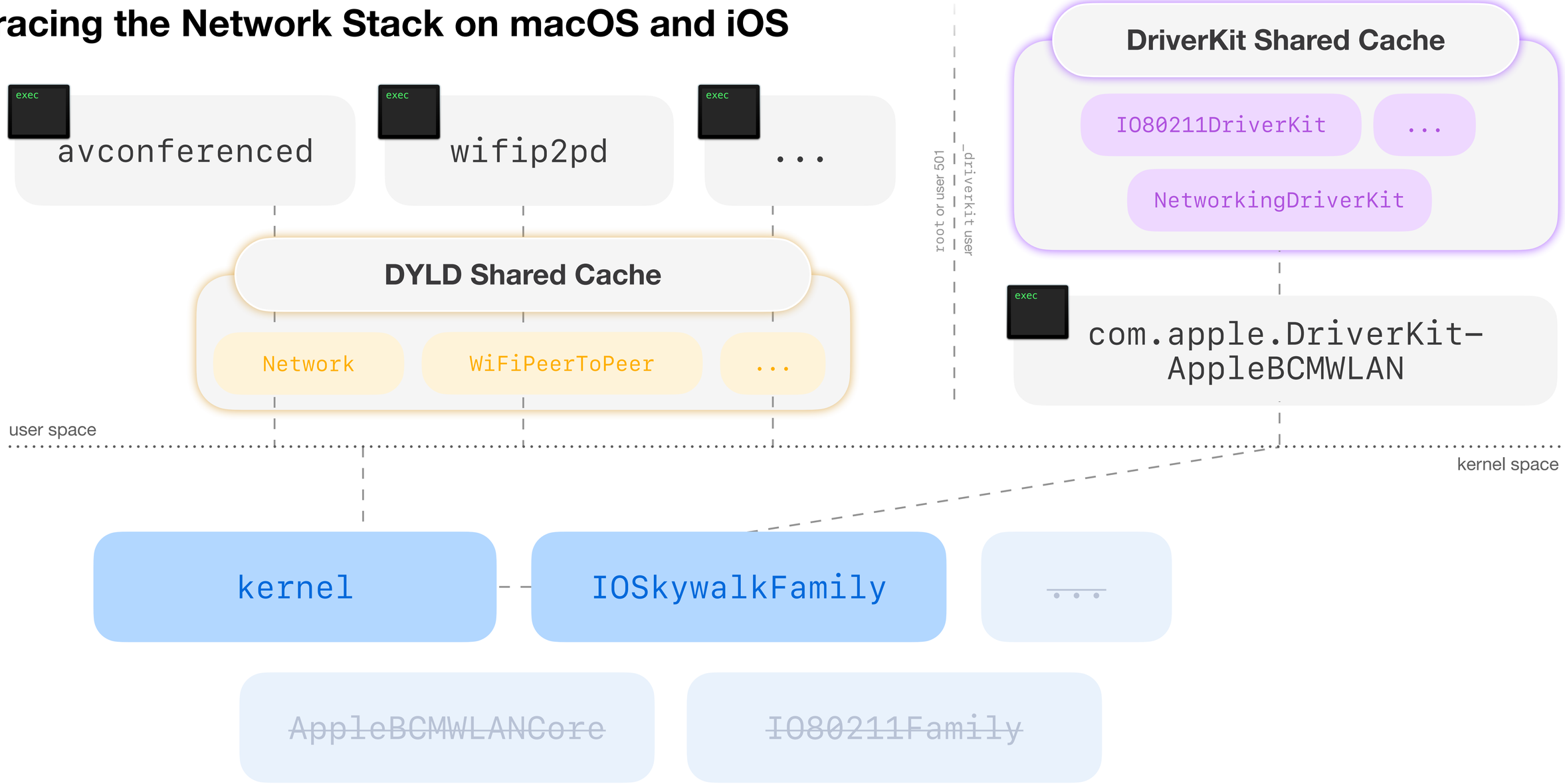
* User space processes (left-hand side) were identified by Jan Röper [A] and Inga Dischinger [B]

Frameworks

DriverKit

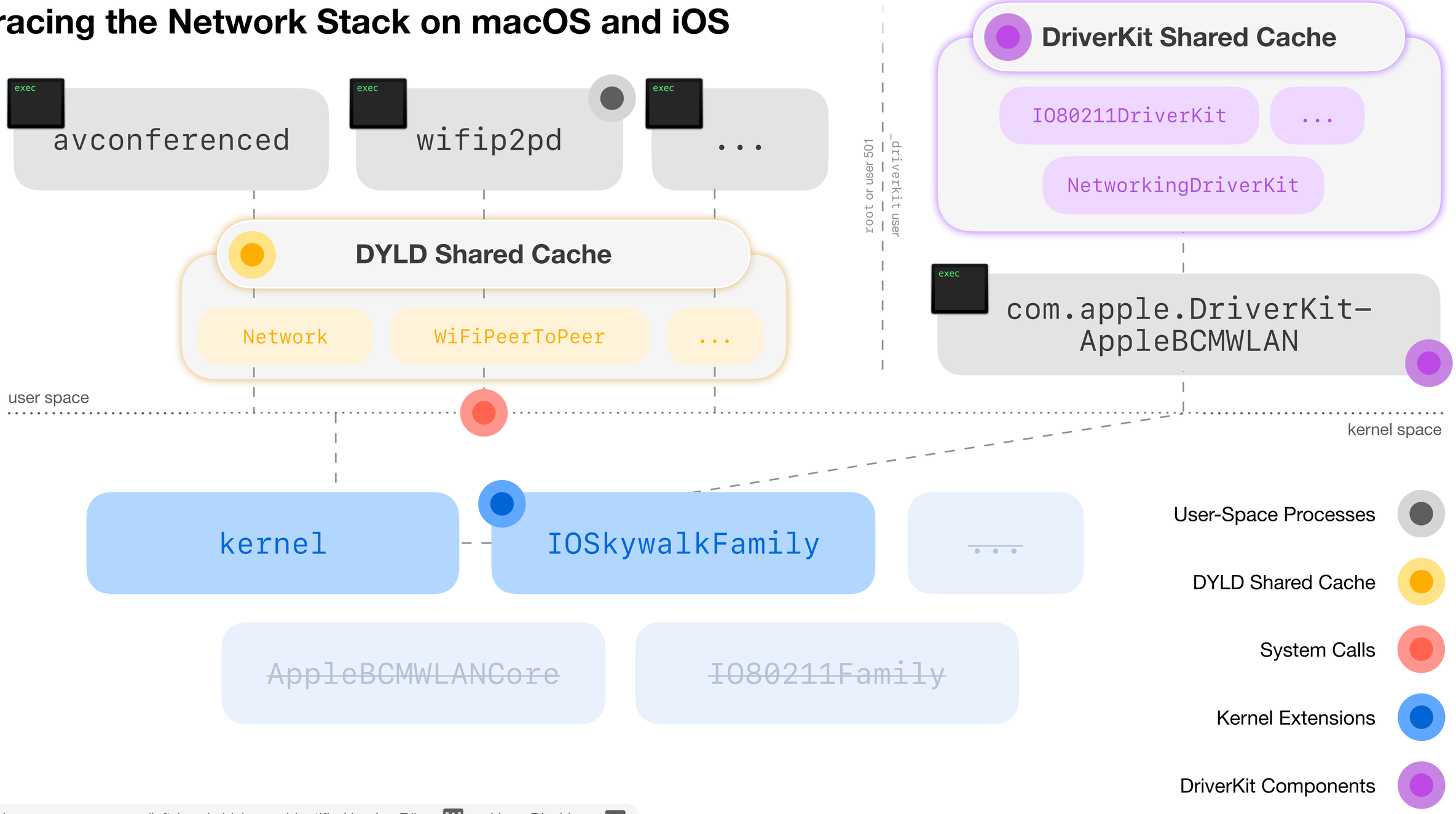
DriverKit-AppleBCMWLAN	Manages interfaces, queues, configures wireless chips; substitutes `AppleBCMWLANCore`
DriverKit	Public Framework providing foundational concepts for interacting with drivers
NetworkingDriverKit	Public Framework for interacting with drivers related to networking
IO80211DriverKit	Handles IEEE 802.11 concepts and states; substitutes `IO80211Family`
core80211DriverKit	Empty (so far?)
BroadcomWLANDriverKit	Empty (so far?)
...	

Tracing the Network Stack on macOS and iOS



* User space processes (left-hand side) were identified by Jan Röper [A] and Inga Dischinger [B]

Tracing the Network Stack on macOS and iOS



* User space processes (left-hand side) were identified by Jan Röper [A] and Inga Dischinger [B]

Network Stack on macOS and iOS

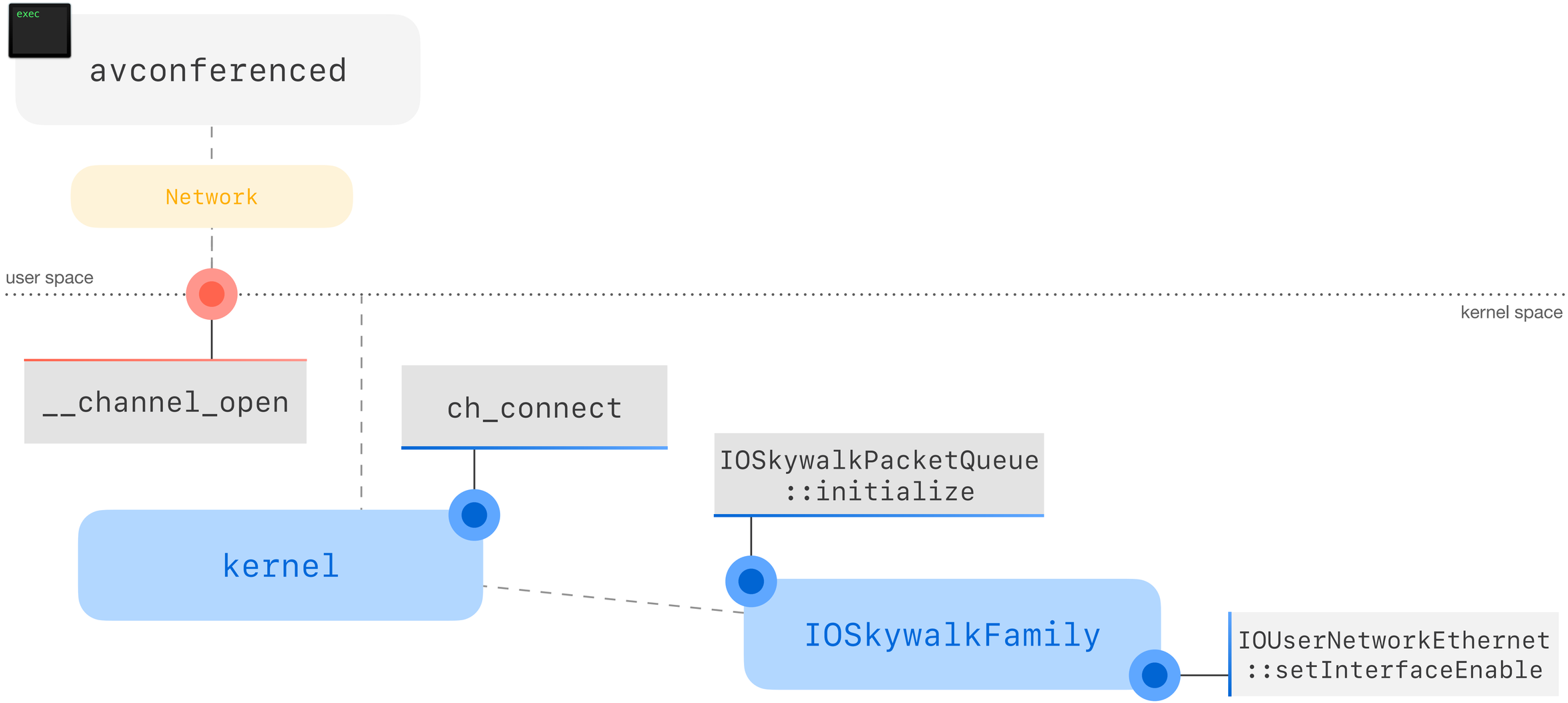
System Components

Interface Lifecycle Management

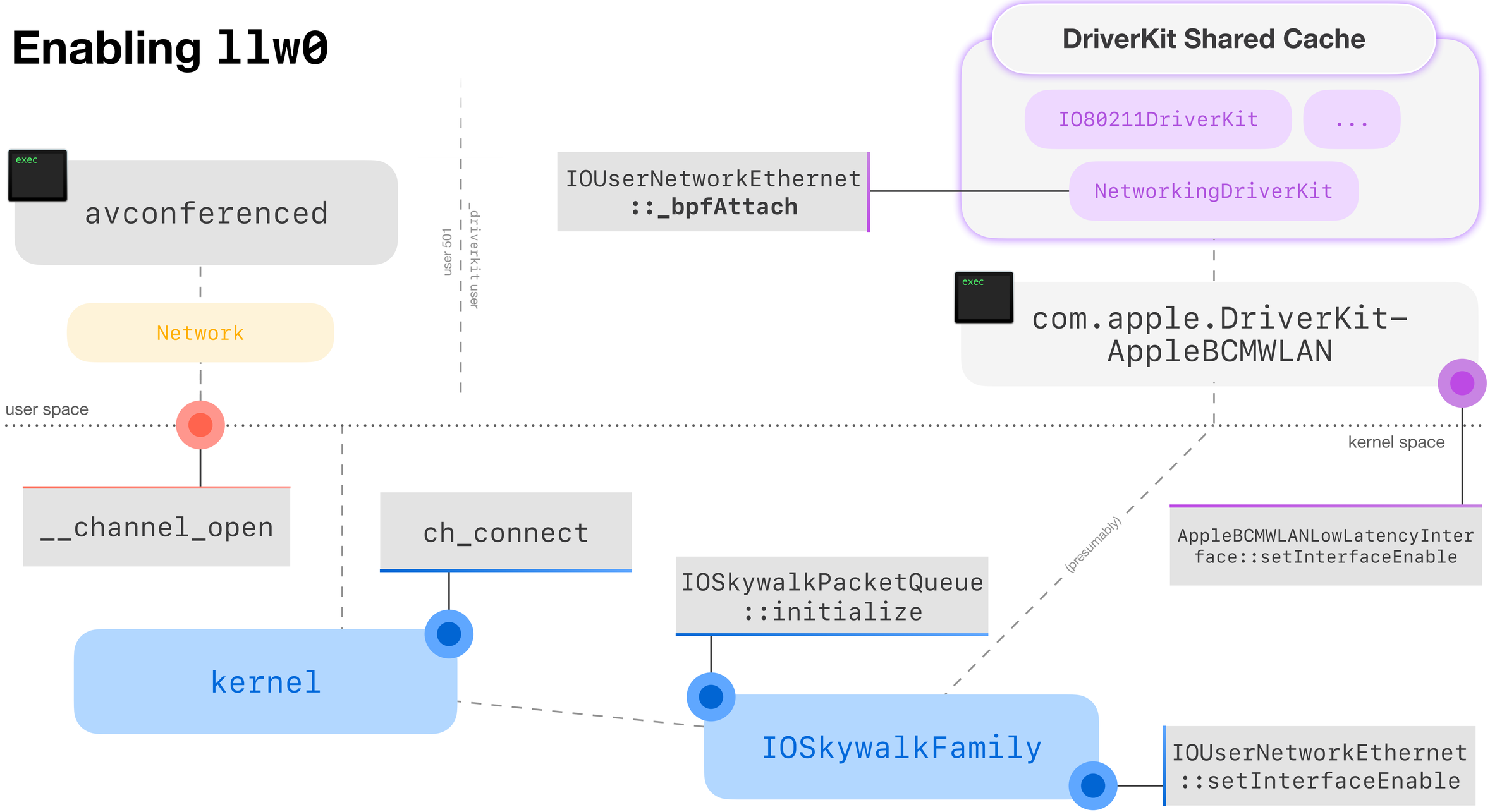
Enabling `llw0`

Enabling `llw0`

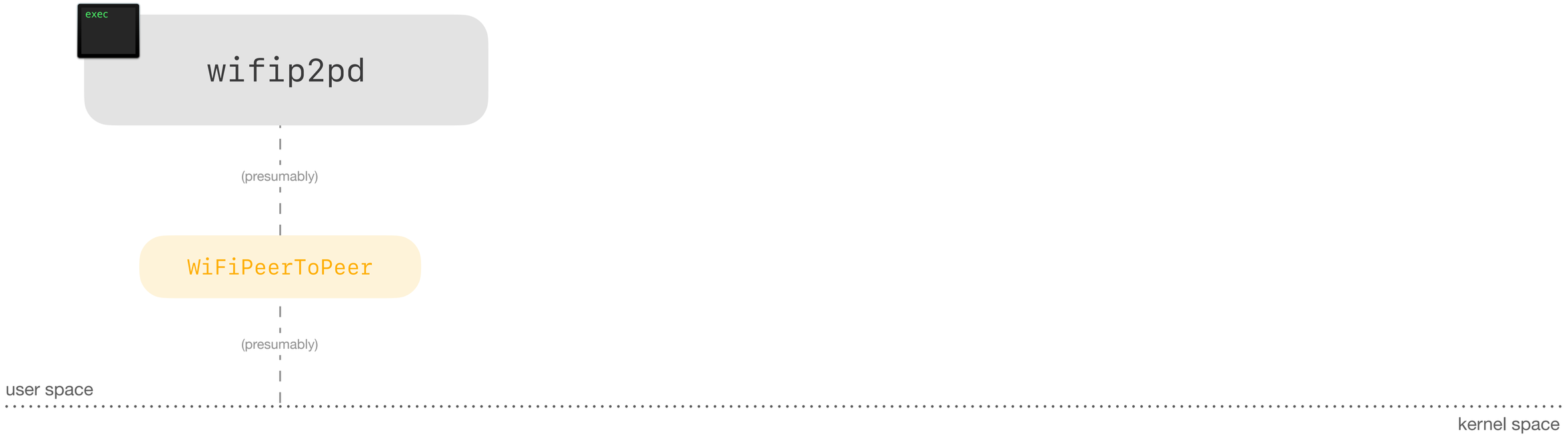
Enabling llw0



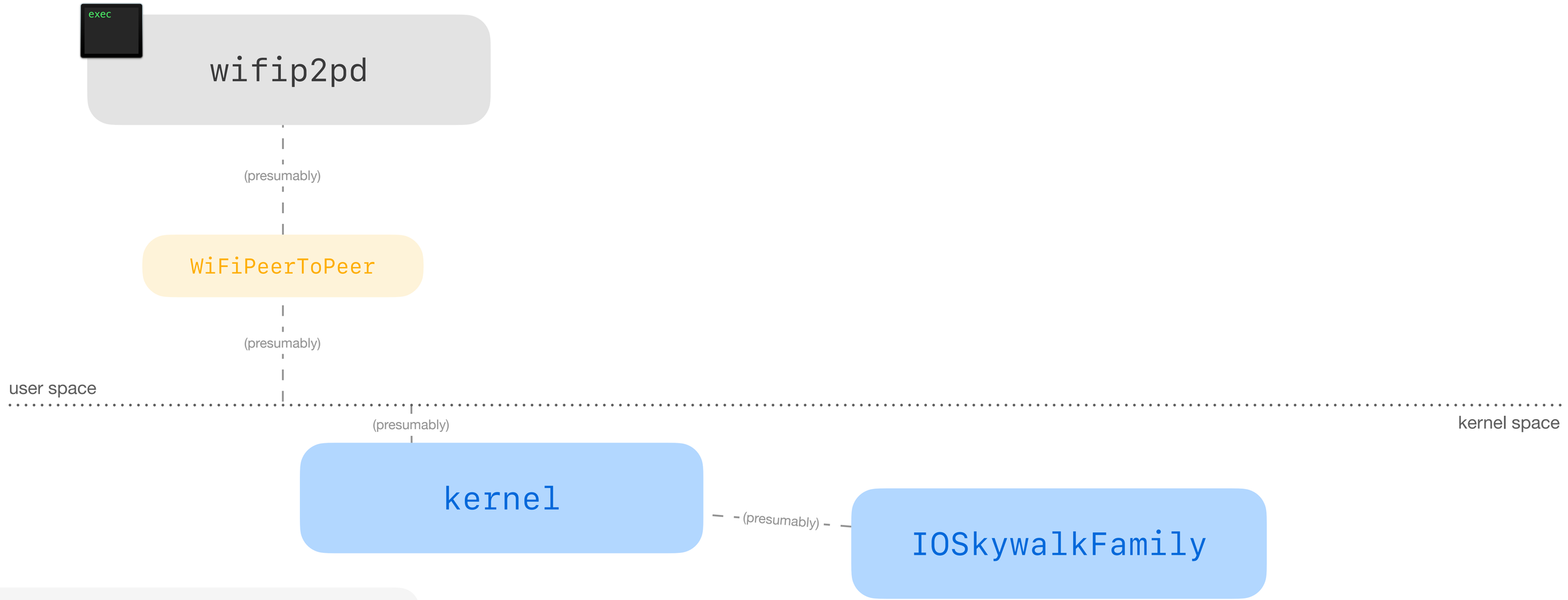
Enabling llw0



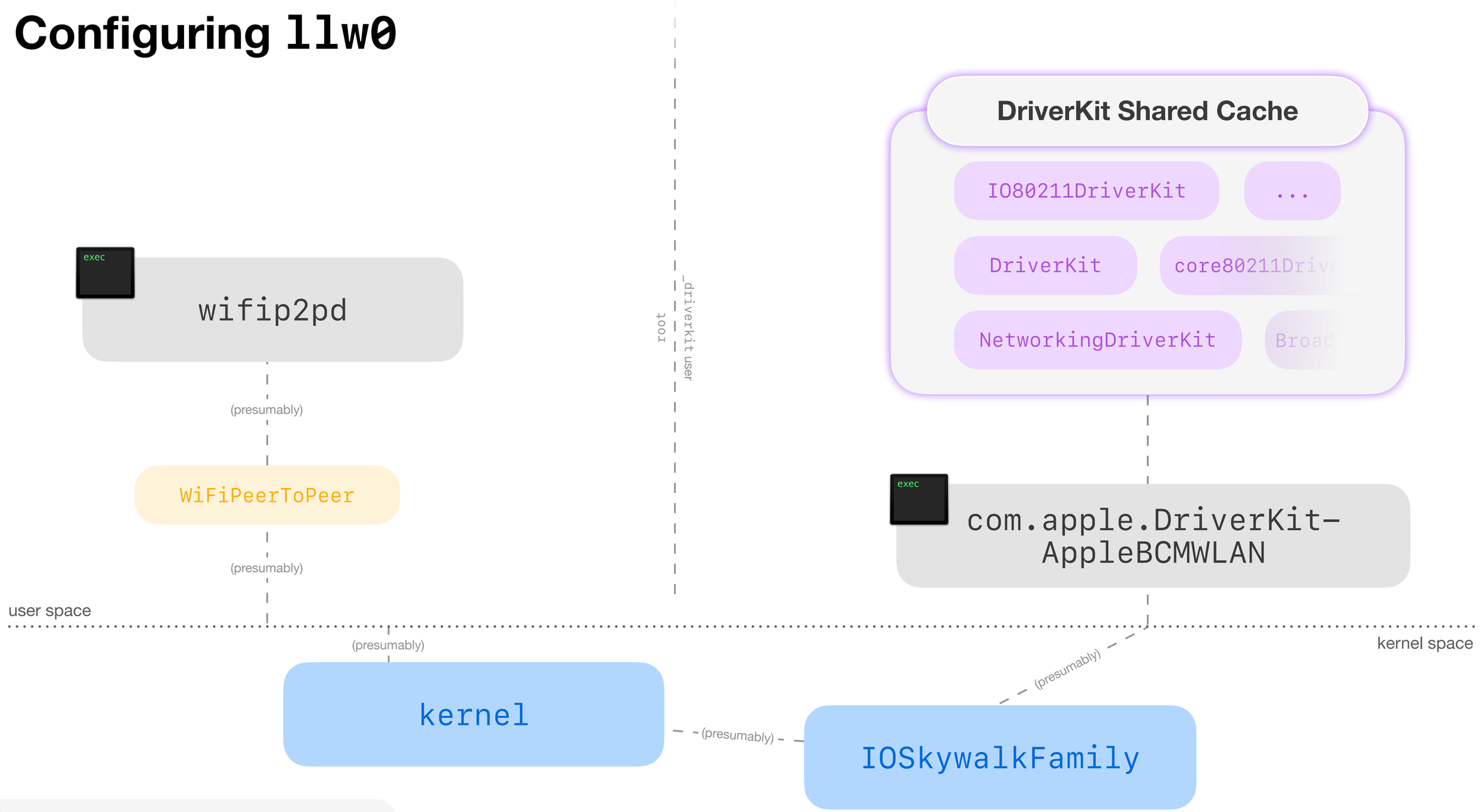
Configuring `llw0`



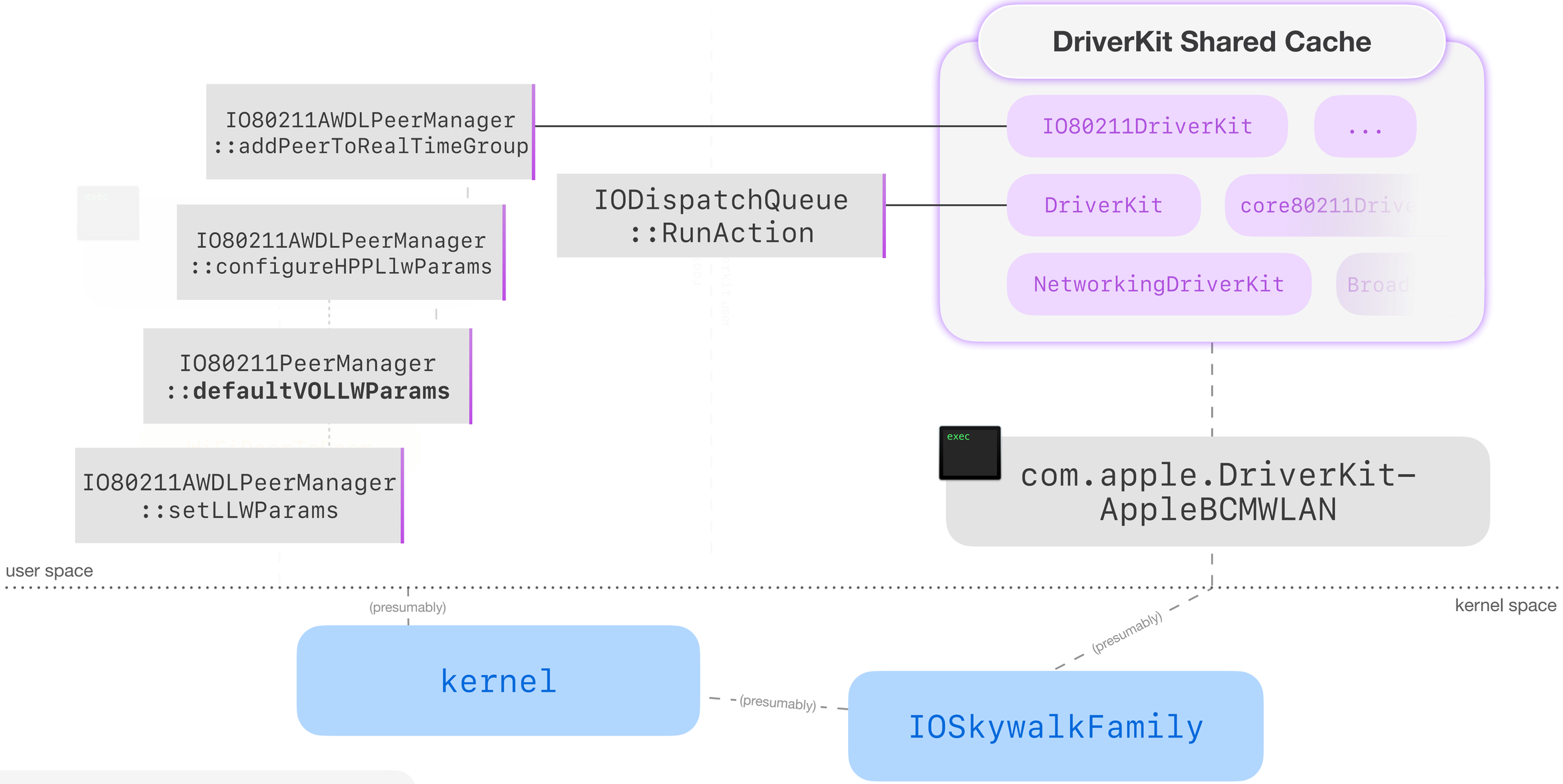
Configuring `llw0`



Configuring `llw0`

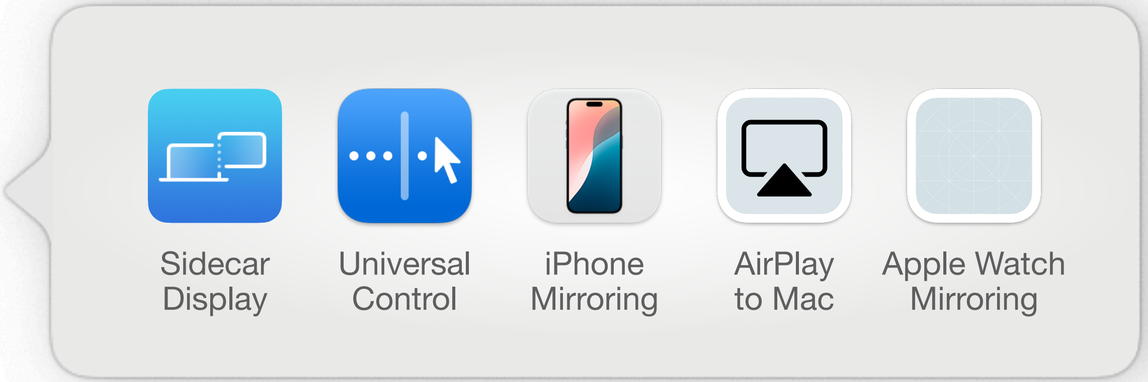


Configuring llw0



Configuring llw0

```
IO80211AWDLPeerManager
::configureHPPLlwParams
```



Configuring llw0

IO80211AWDLPeerManager
::addPeerToRealTimeGroup

IO80211AWDLPeerManager
::configureHPPLlwParams

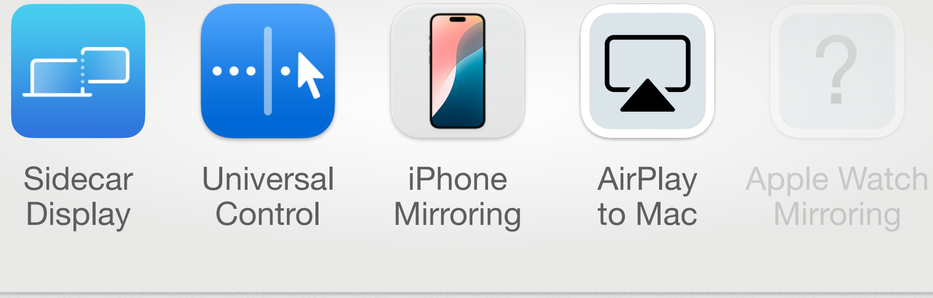
IO80211AWDLPeerManager
::setLLWParams

IO80211PeerManager
::defaultVOLLWParams

DriverKit Shared Cache

IO80211DriverKit

IODispatchQueue



user space

kernel space

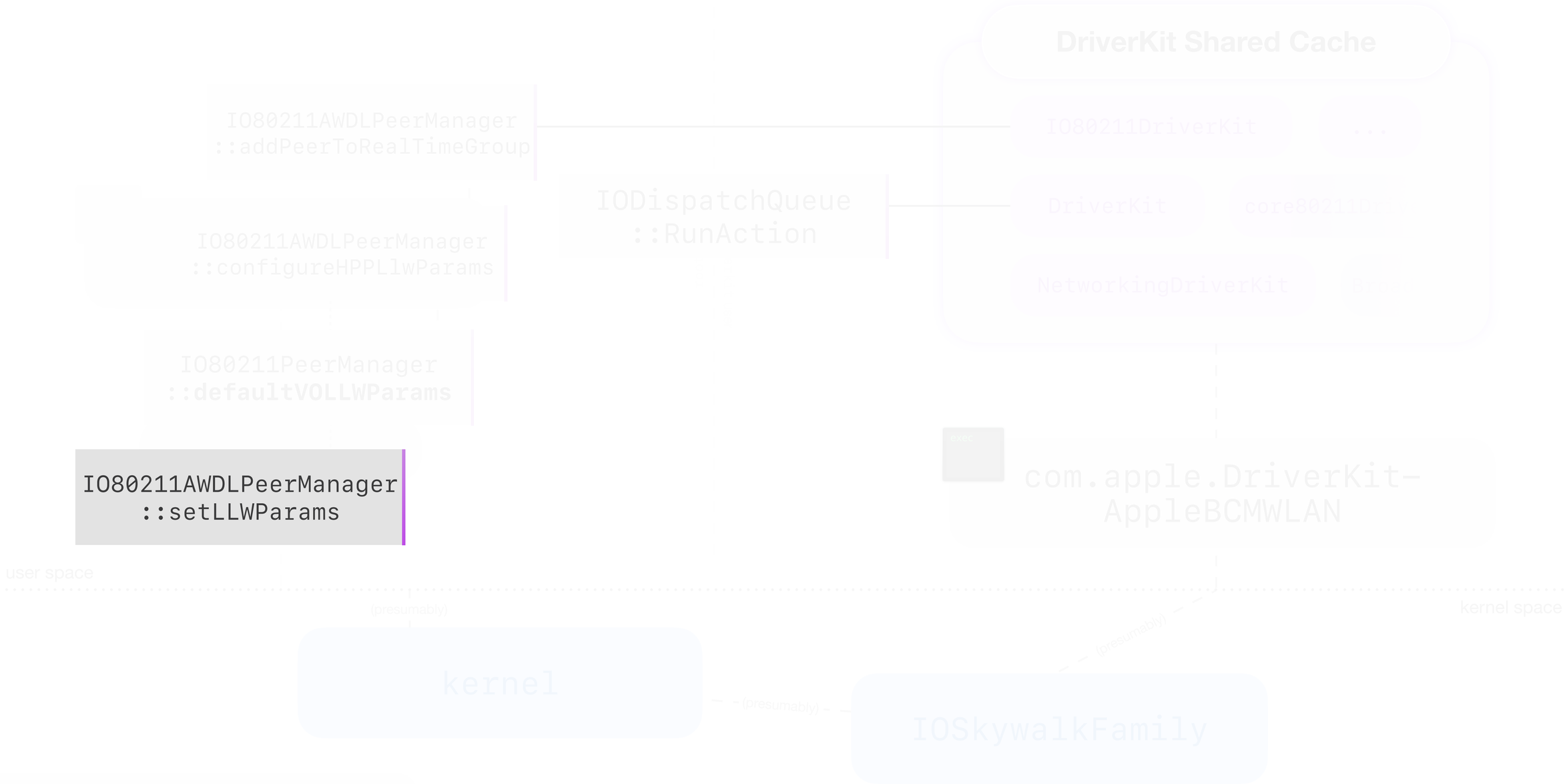
(presumably)

kernel

(presumably)

IOSkywalkFamily

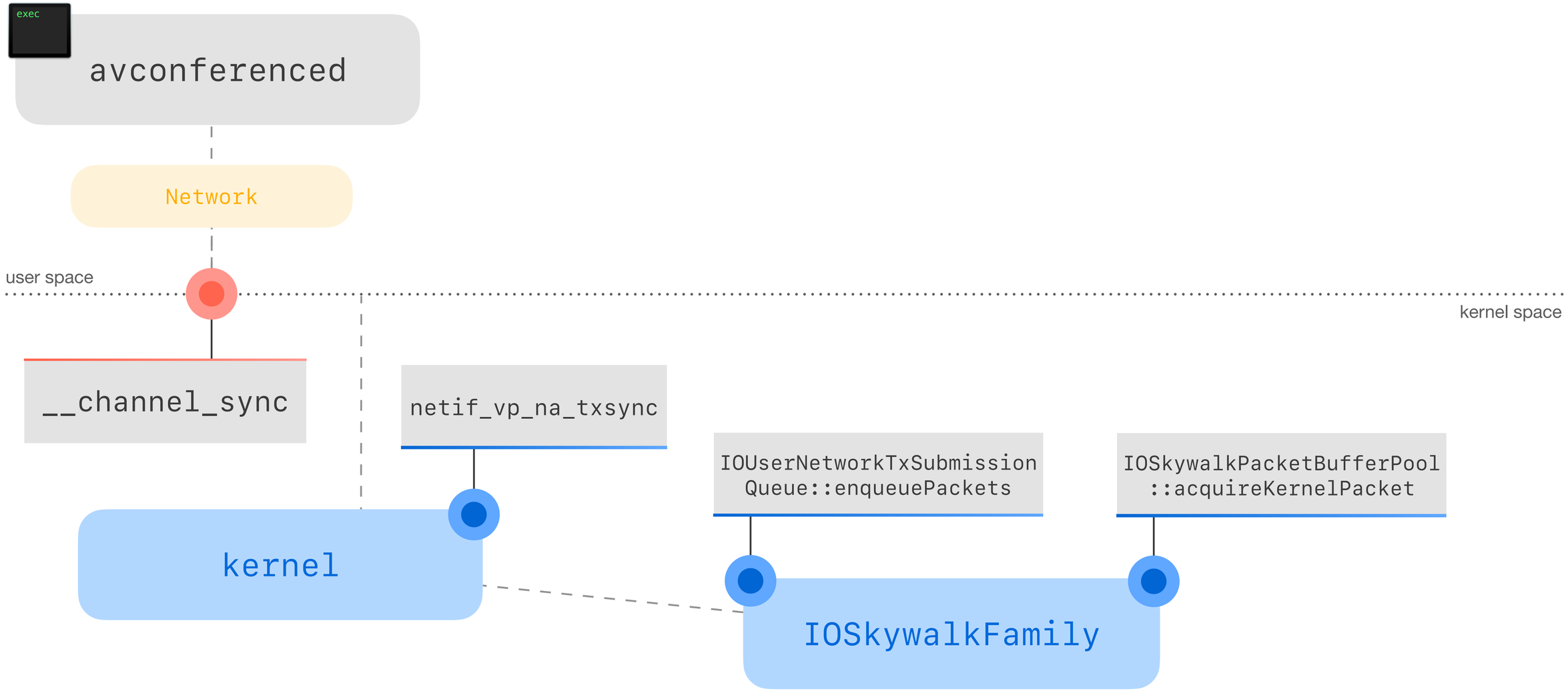
Configuring llw0



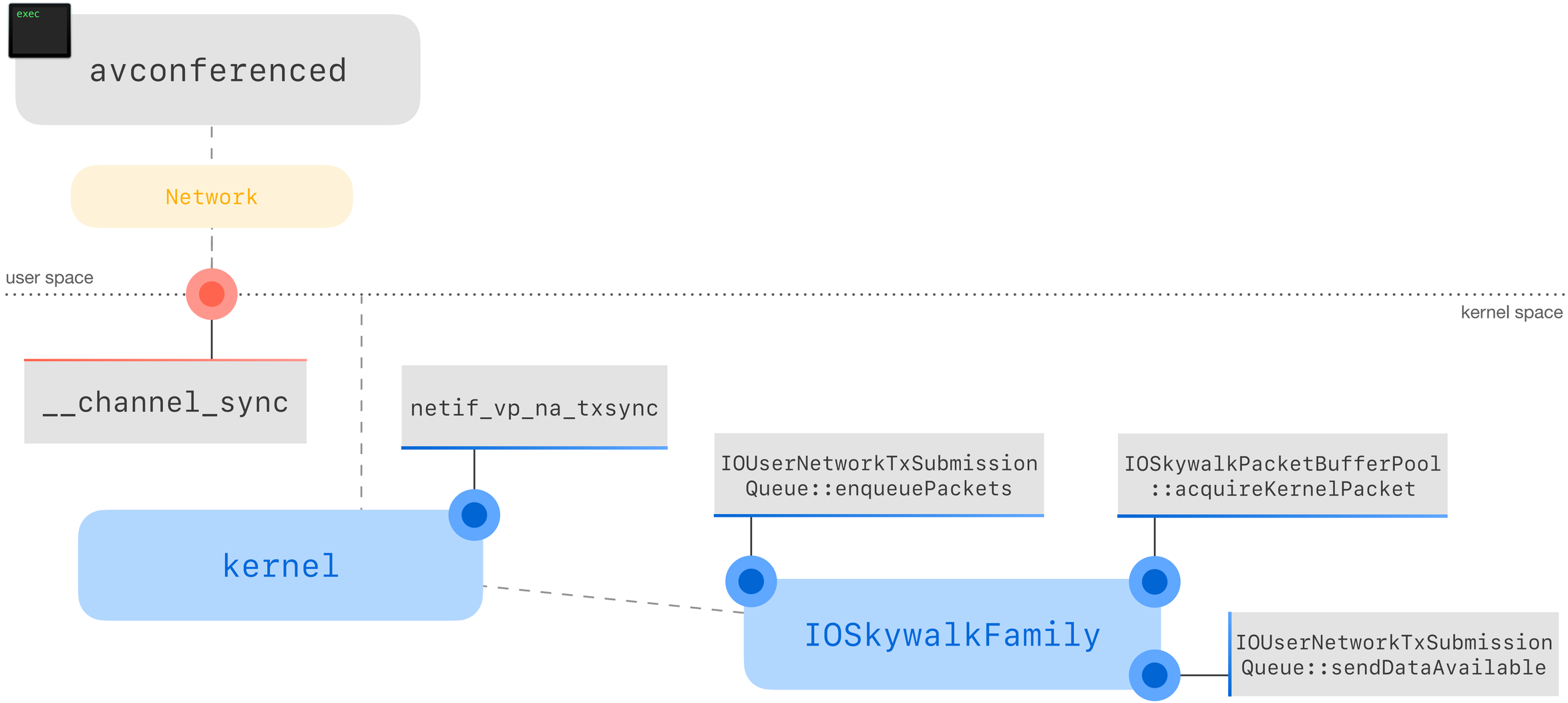
Transmitting via `llw0`

Transmitting via `llw0`

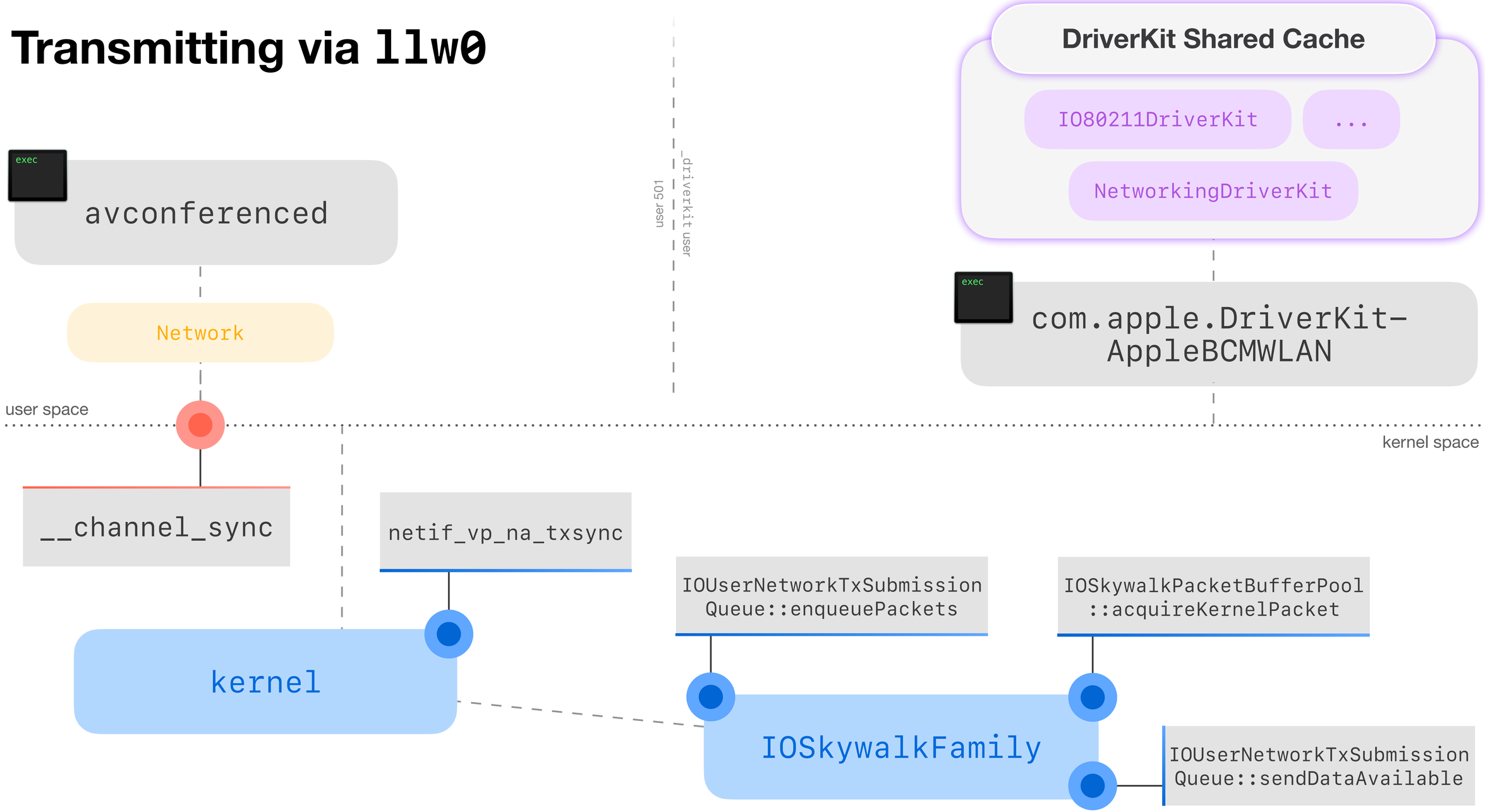
Transmitting via `llw0`



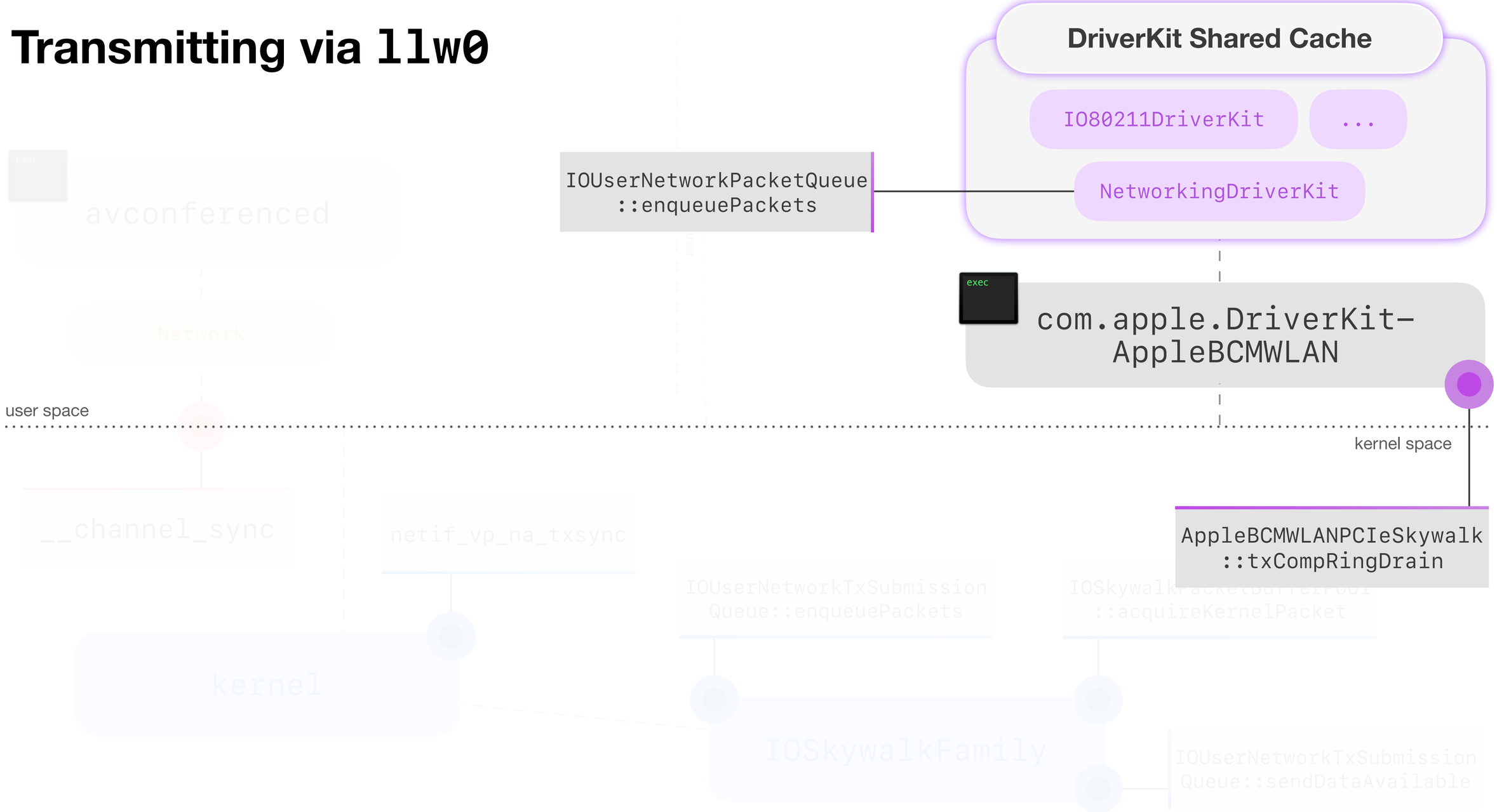
Transmitting via `llw0`



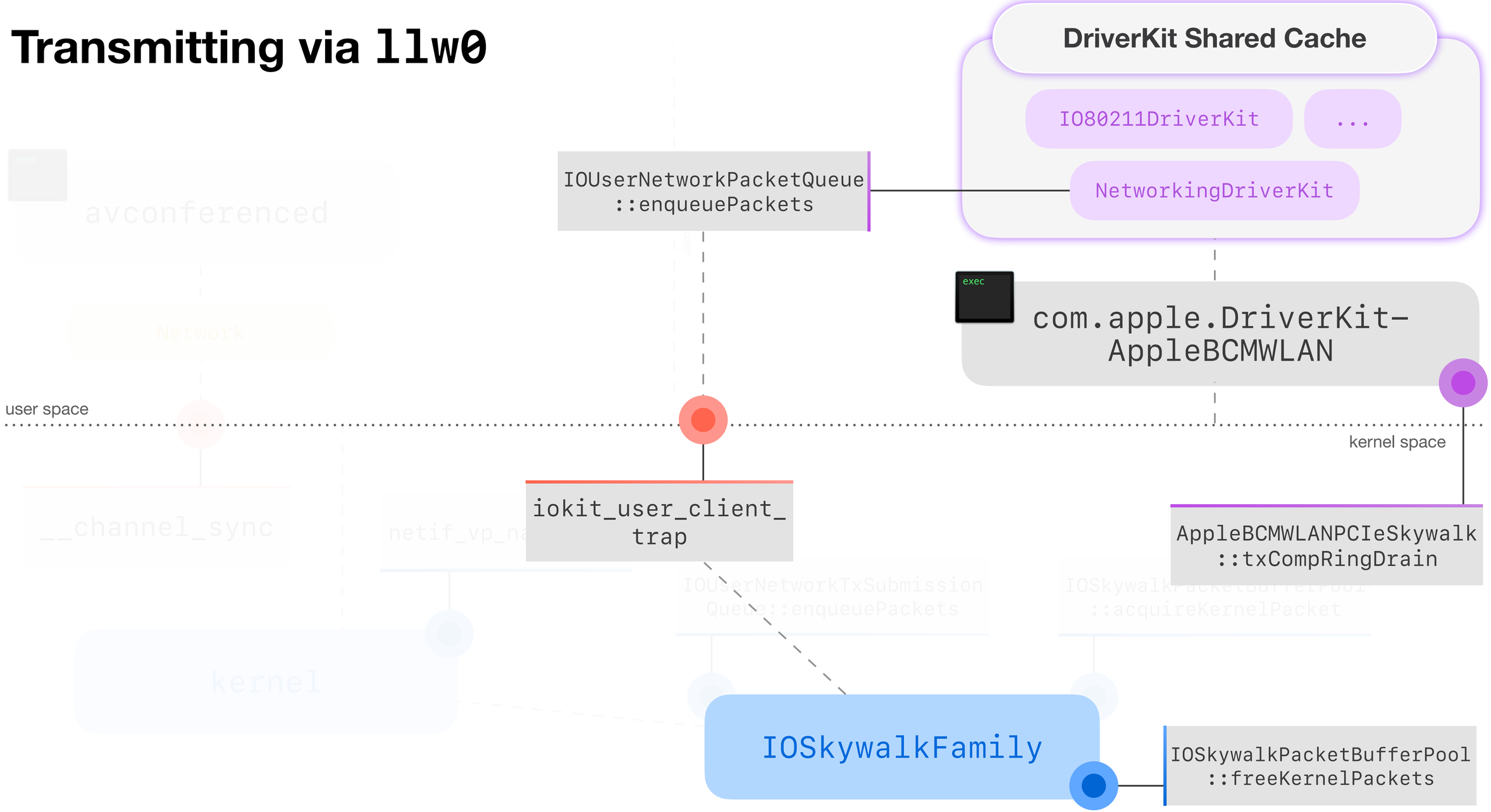
Transmitting via `llw0`



Transmitting via `llw0`



Transmitting via `llw0`



DYLD Shared Cache

Network

WiFiPeerToPeer

exec

avconferenced

exec

wifip2pd

DriverExtension

exec

com.apple.DriverKit-AppleBCMWLAN

Berkley Packet Filter

User Packet Pool

__channel_sync

__channel_open

System Components Involved in Data Transmission with Low-Latency WiFi

- User-Space Processes
- DYLD Shared Cache
- System Calls
- DriverKit Components
- Kernel Extensions

NVMe

Completion Queues | Submission Queues

in transmit and receive direction

kernel

IOSkywalk Family

DriverKit Shared Cache

IO80211DriverKit

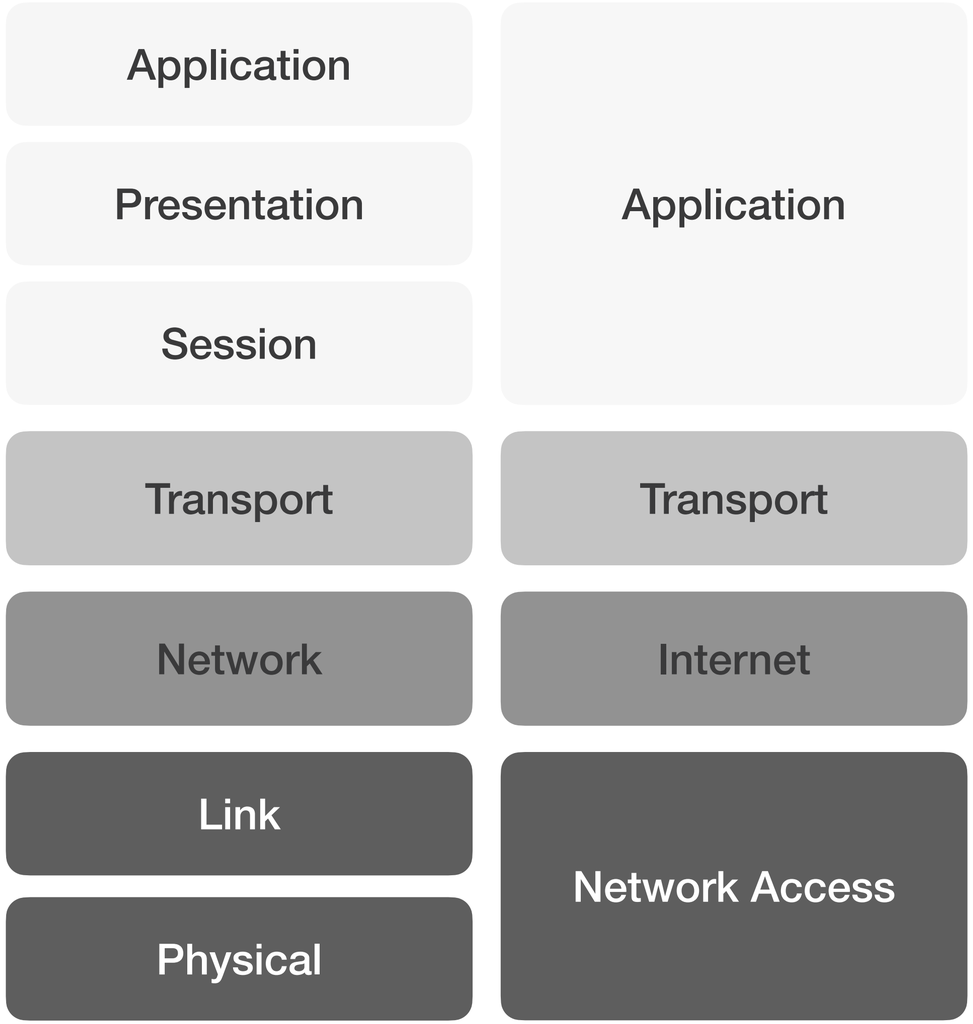
...

NetworkingDriverKit

Log Aggregator

Network Stack on macOS and iOS

Low-Latency in LLW

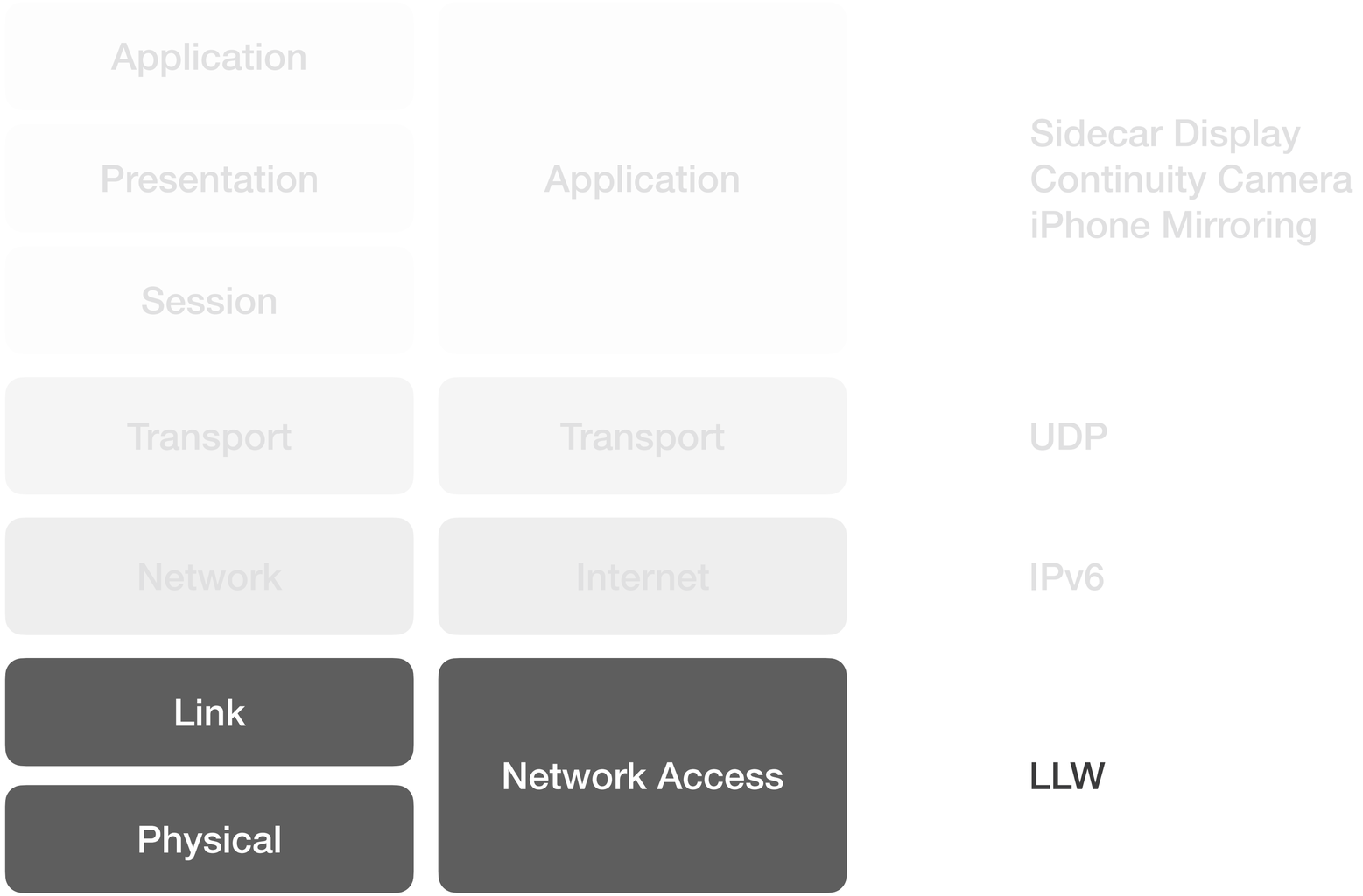


Sidecar Display
Continuity Camera
iPhone Mirroring

UDP

IPv6

LLW


Application
Presentation
Session
Application
Transport
Transport
Network
Internet
Link
Physical
Network Access
Sidecar Display
Continuity Camera
iPhone Mirroring
UDP
IPv6
LLW

Low-Latency in LLW

IEEE 802.11e/n/ac Details

Hardware Capabilities

IEEE 802.11e

Quality of Service

Enhanced **D**istributed **C**hannel **A**ccess

- Access Categories
- **A**rbitration **I**nter-**F**rame **S**pacing
- **C**ontention **W**indow (max, min)
- Transmission Opportunity (**TXOP**)

Block **A**cknowledgement

IEEE 802.11n

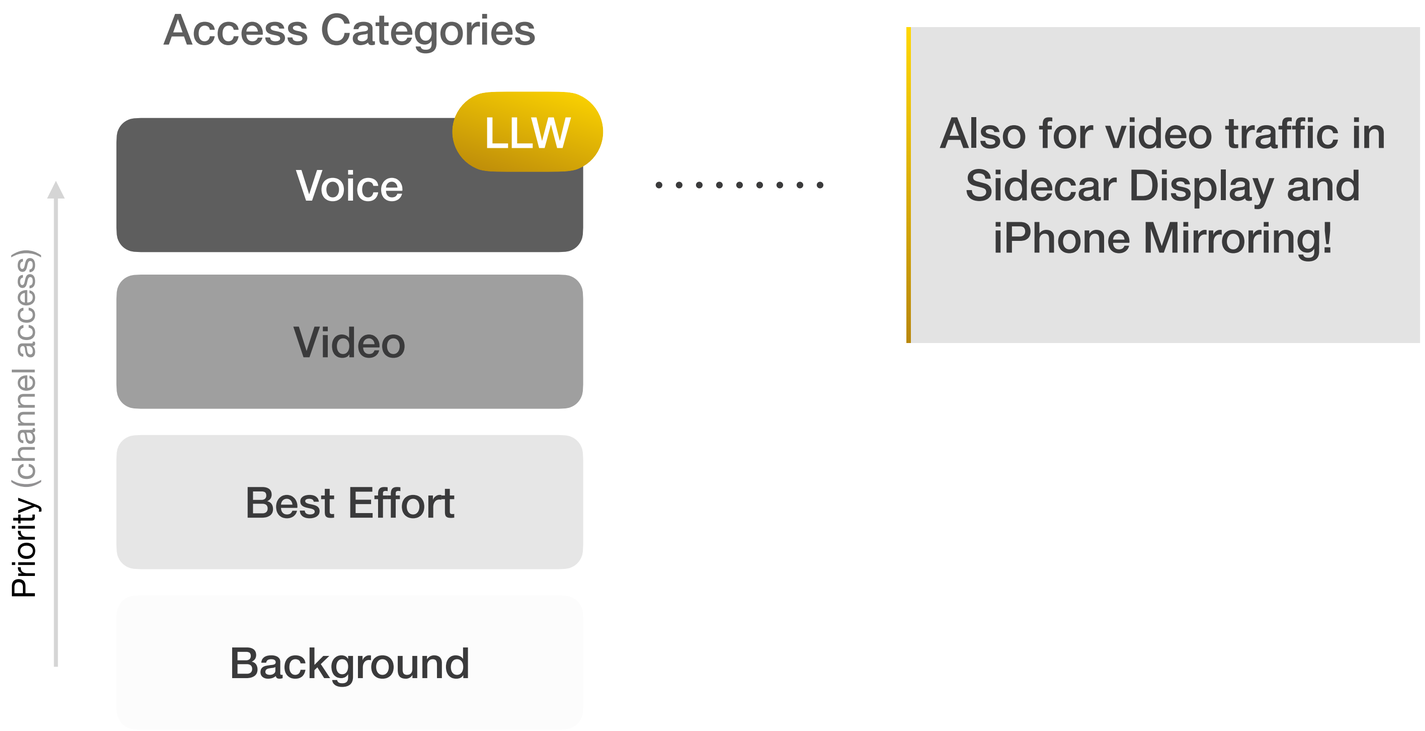
High Throughput

- Aggregated **MSDU**
- Aggregated **MPDU**
- **R**everse **D**irection **G**rant

[Q] [R]

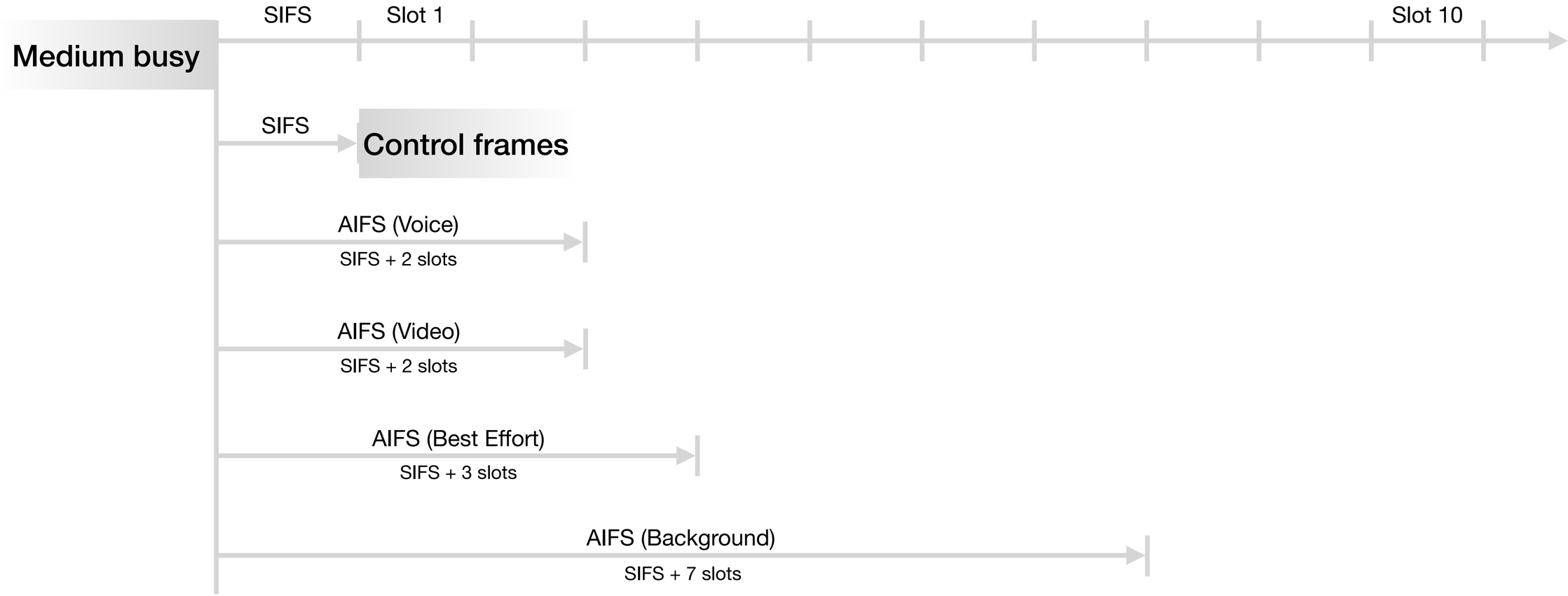
Enhanced Distributed Channel Access

IEEE 802.11e Concepts



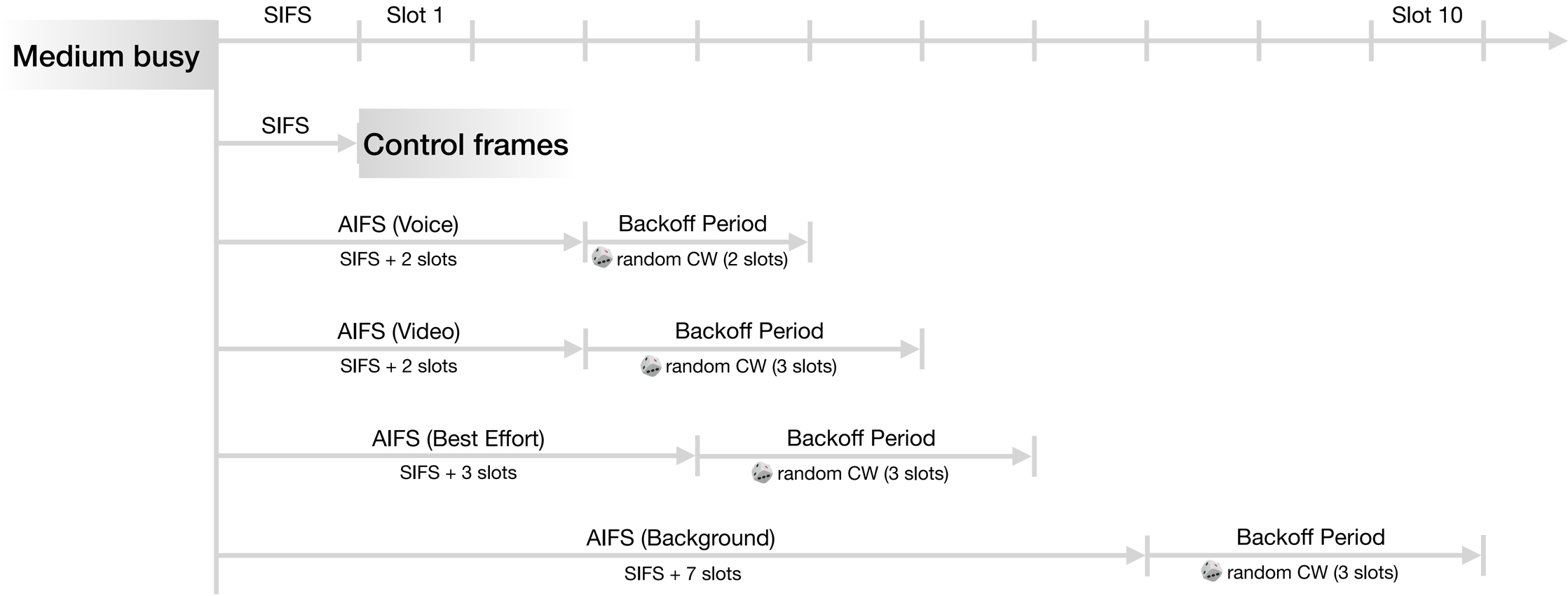
Enhanced Distributed Channel Access

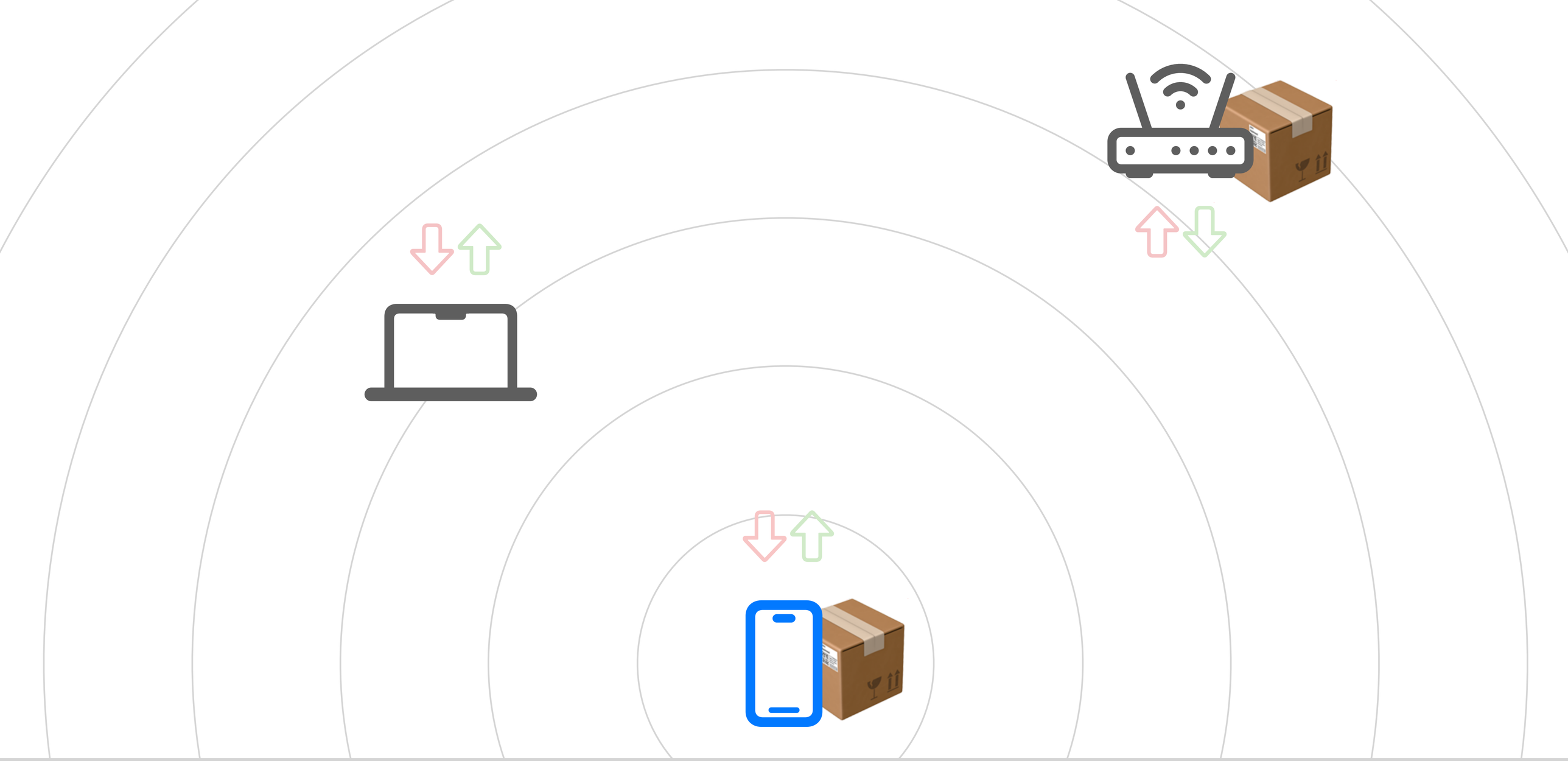
IEEE 802.11e Concepts



Enhanced Distributed Channel Access

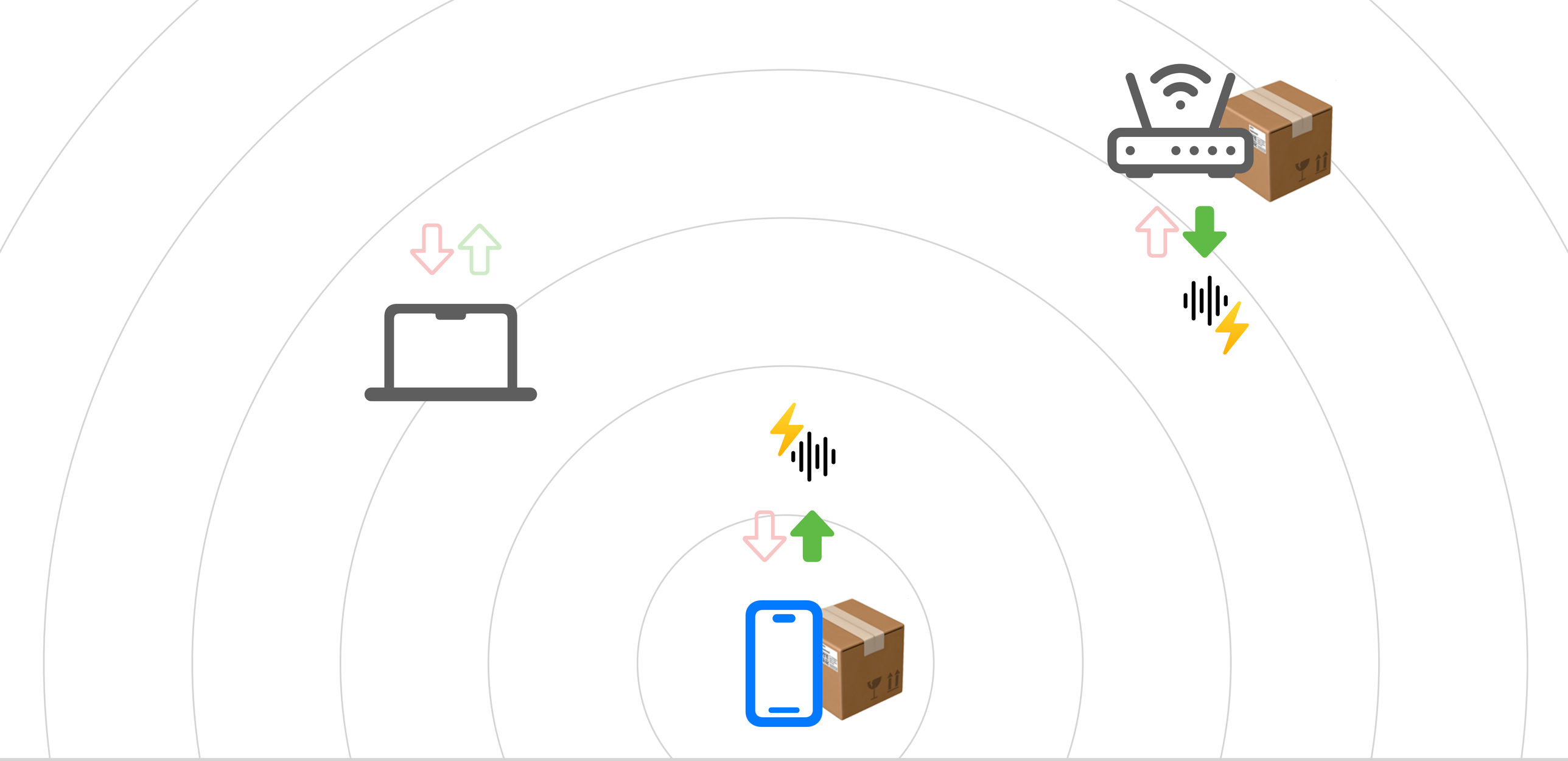
IEEE 802.11e Concepts





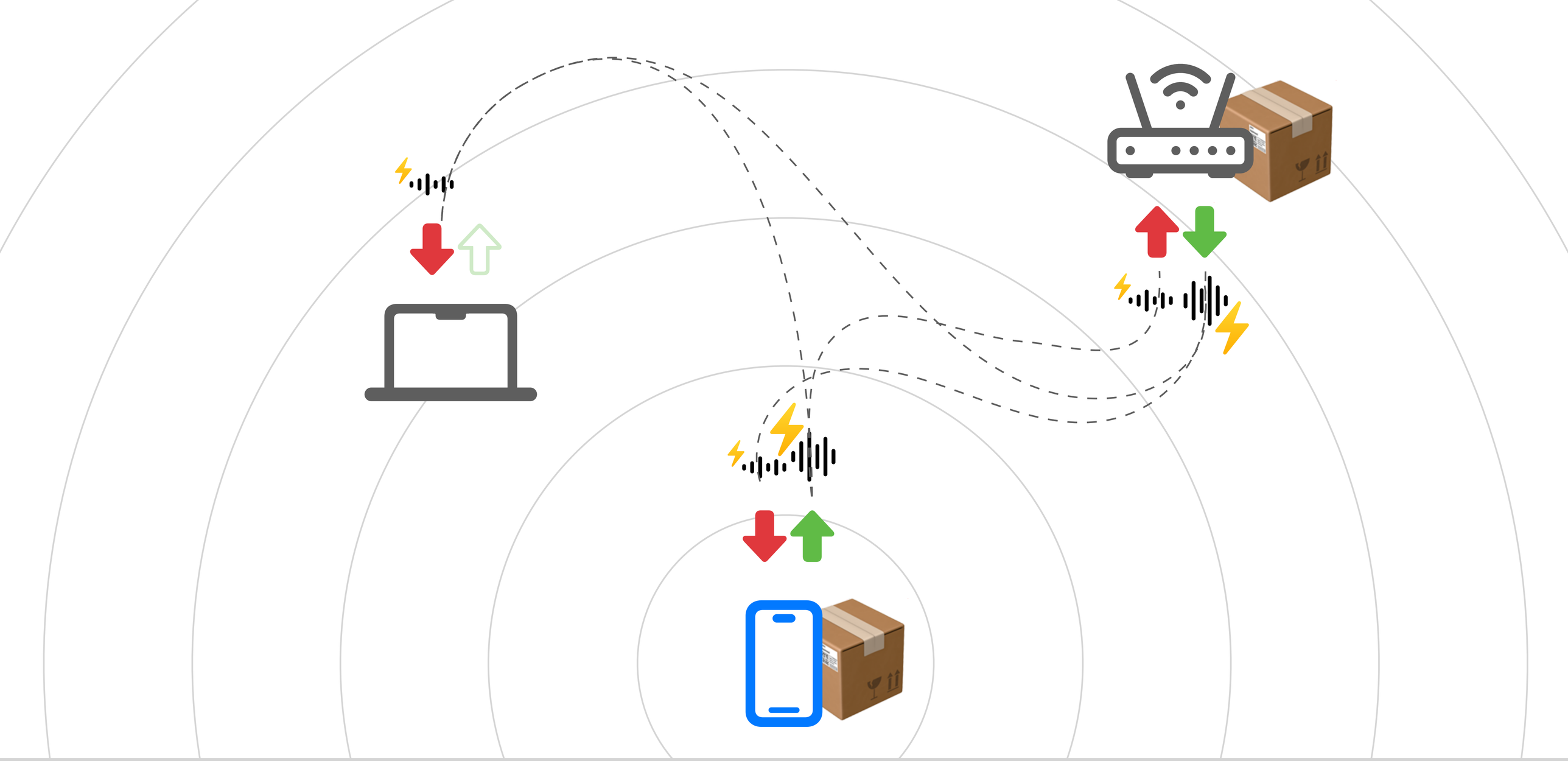
Problem

No collision *detection* due to half-duplex transceivers.



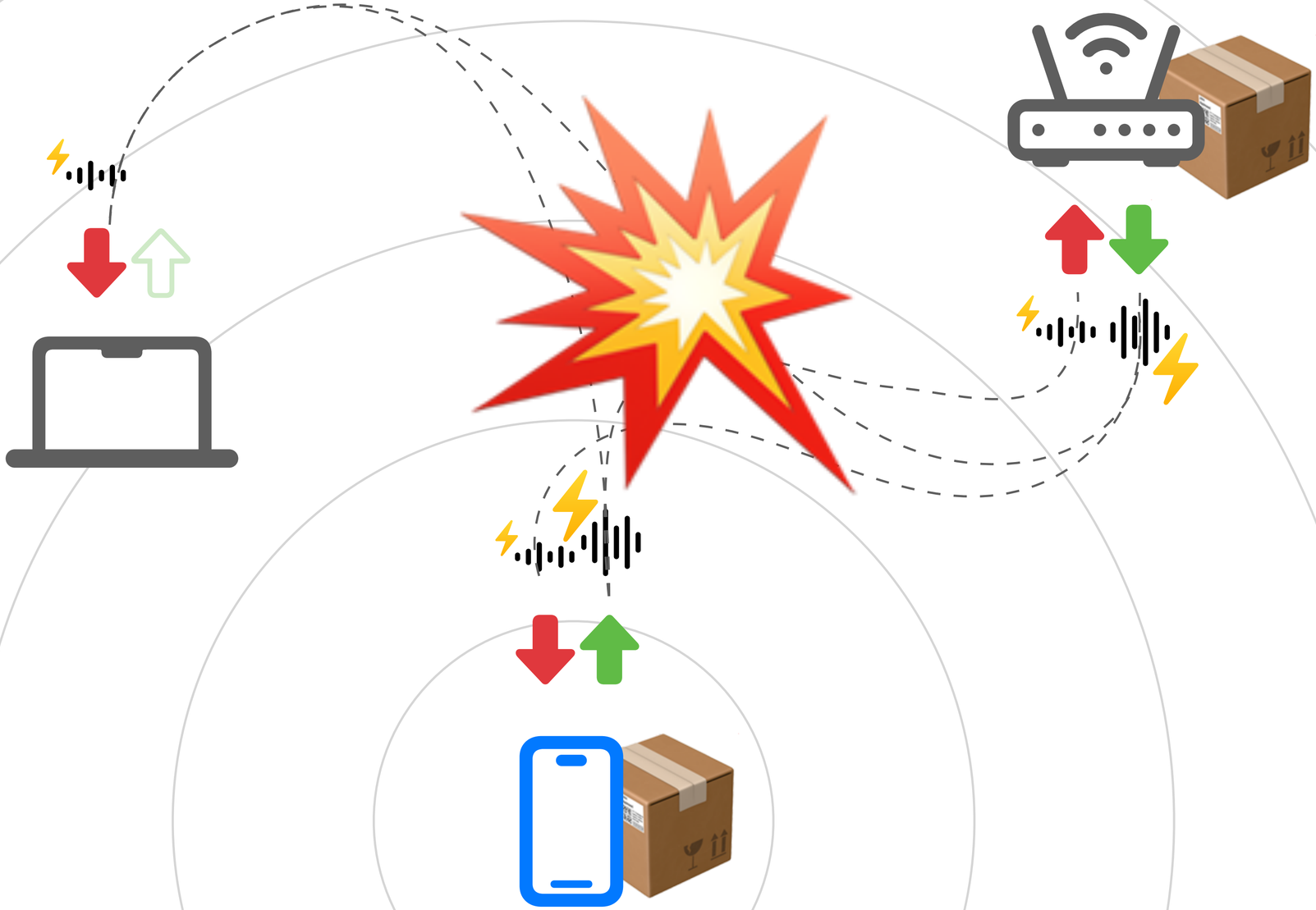
Problem

No collision *detection* due to half-duplex transceivers.



Problem

No collision *detection* due to half-duplex transceivers.



Problem

No collision *detection* due to half-duplex transceivers.

[0; CWmin]

[0; CWmin]

Problem

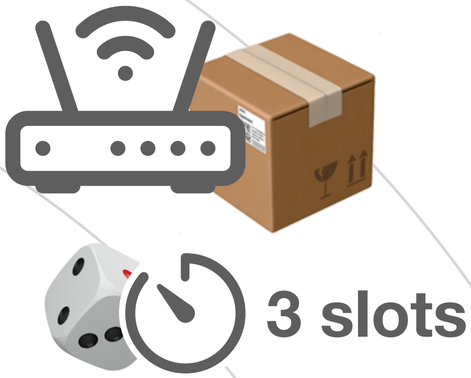
No collision *detection* due to half-duplex transceivers.

Solution

Randomize medium access to avoid collisions.

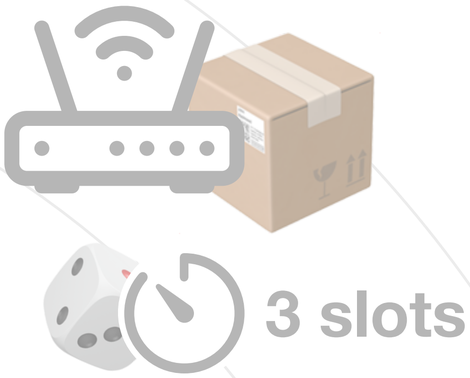
Problem
No collision *detection* due to half-duplex transceivers.

Solution
Randomize medium access to avoid collisions.



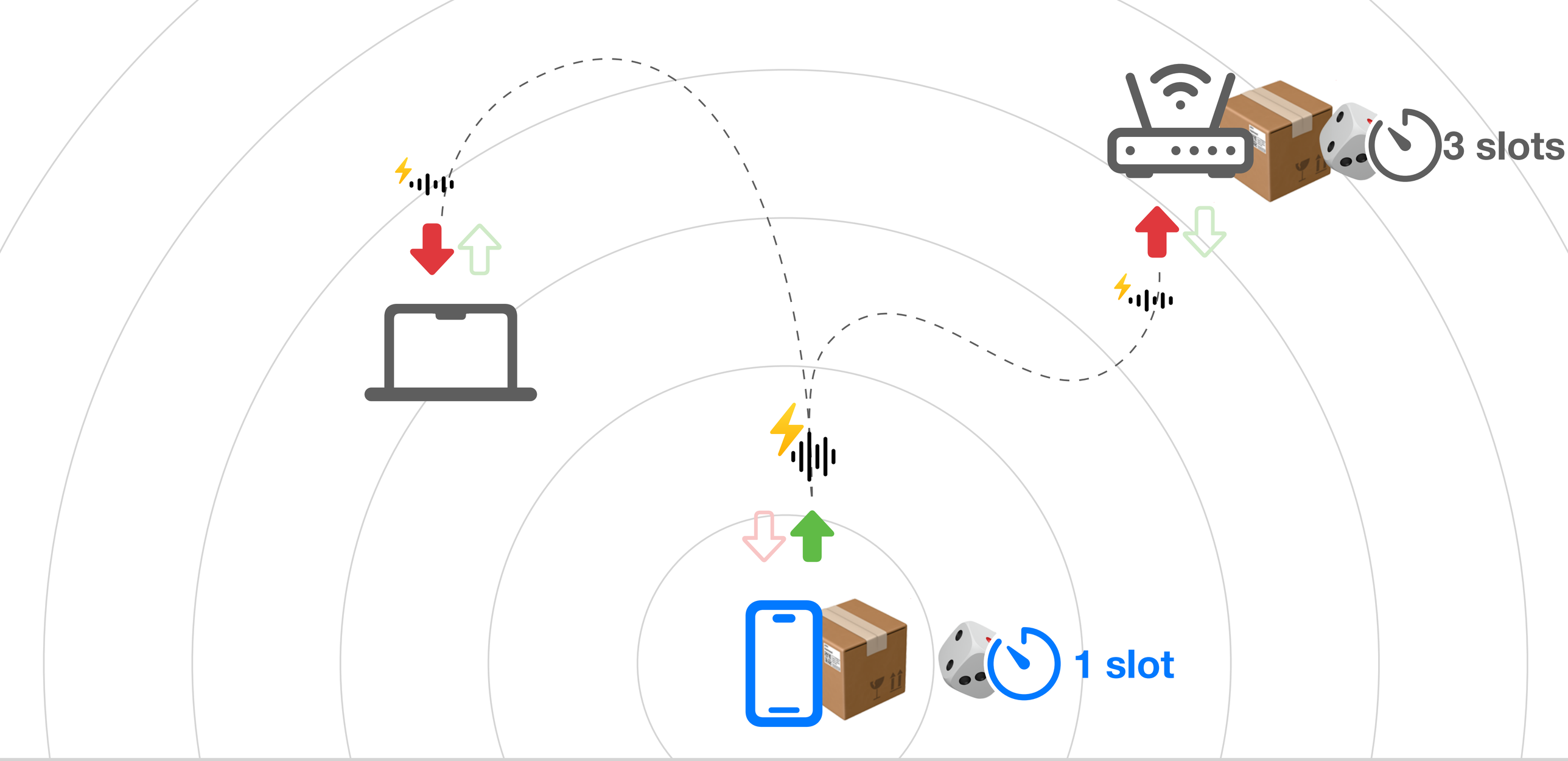
Problem
No collision *detection* due to half-duplex transceivers.

Solution
Randomize medium access to avoid collisions.



Problem
No collision *detection* due to half-duplex transceivers.

Solution
Randomize medium access to avoid collisions.

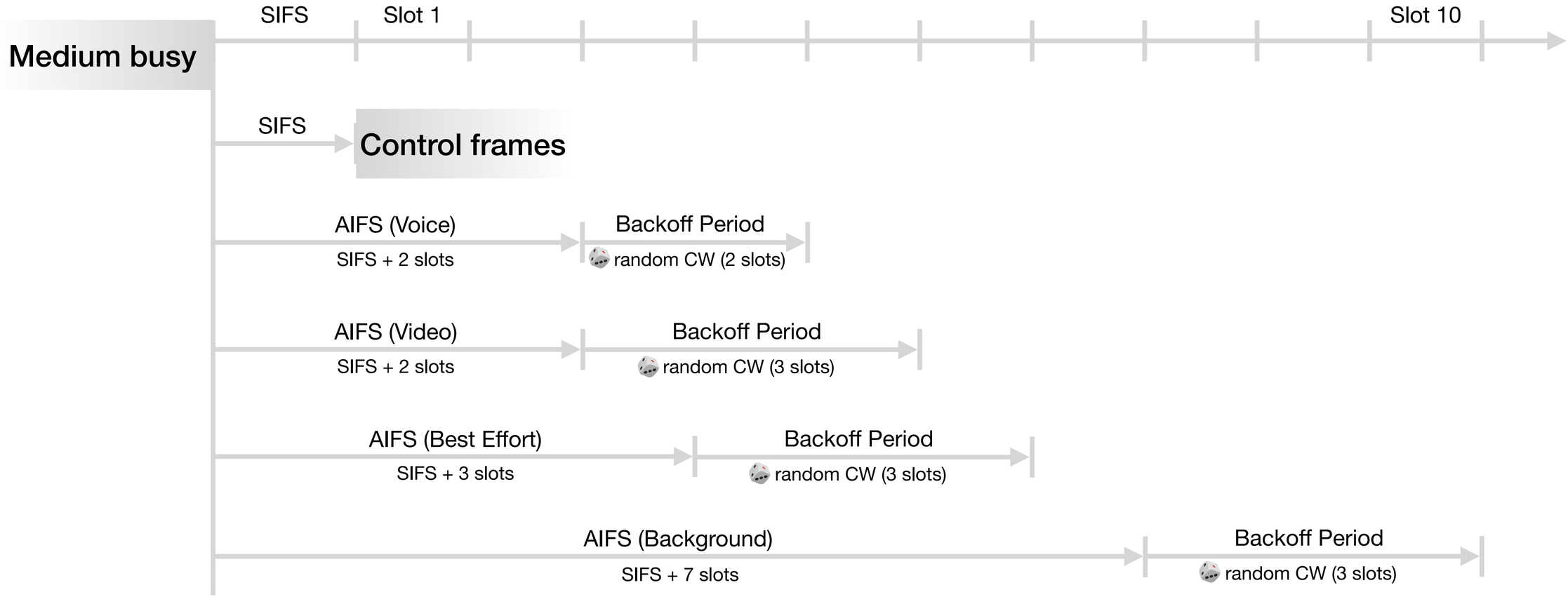


Problem
No collision *detection* due to half-duplex transceivers.

Solution
Randomize medium access to avoid collisions.

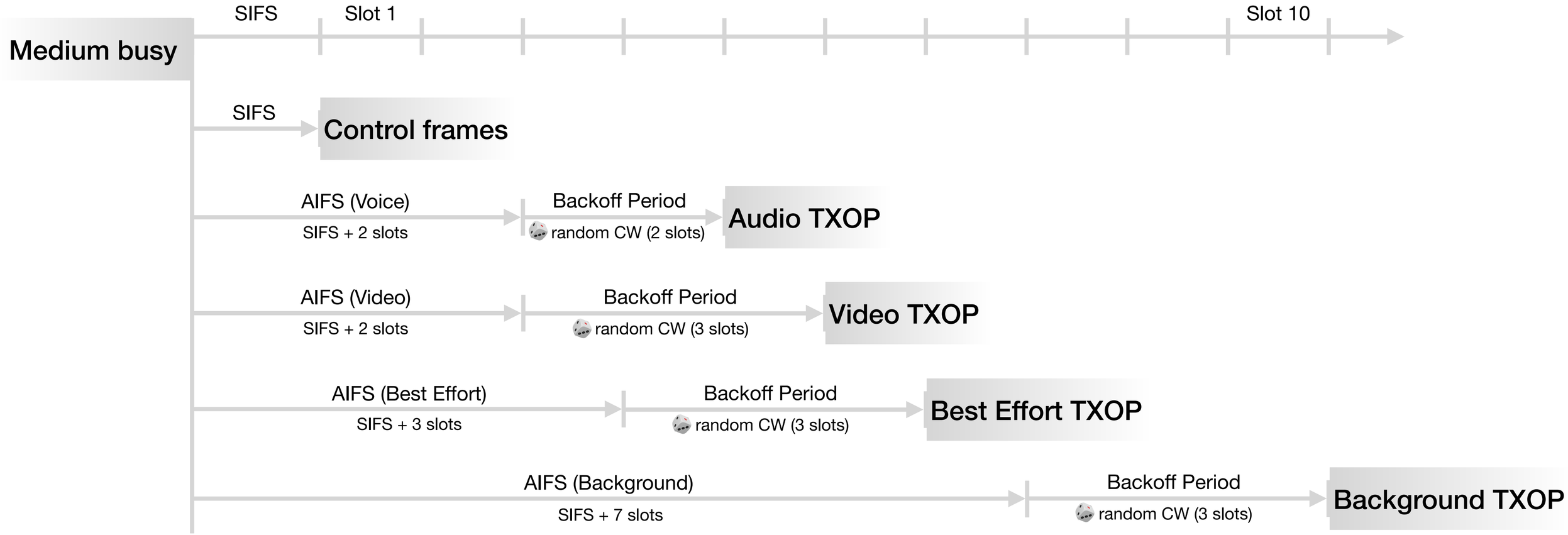
Enhanced Distributed Channel Access

IEEE 802.11e Concepts



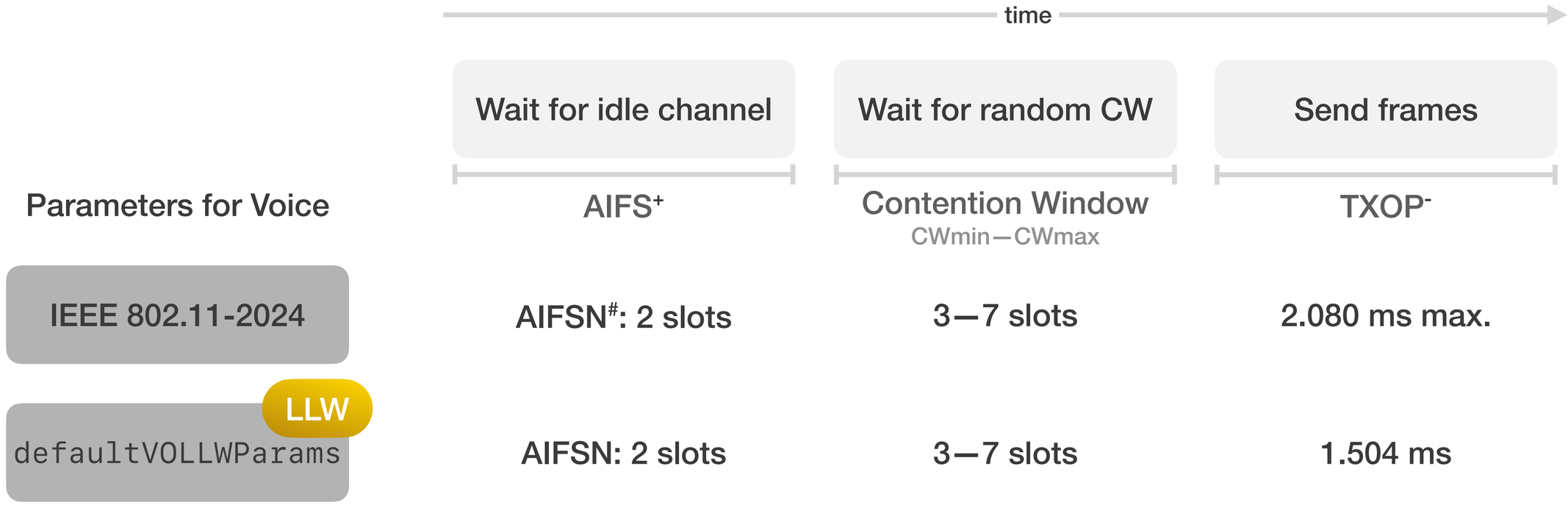
Enhanced Distributed Channel Access

IEEE 802.11e Concepts



LLW Parameters

IEEE 802.11e Concepts



[U]

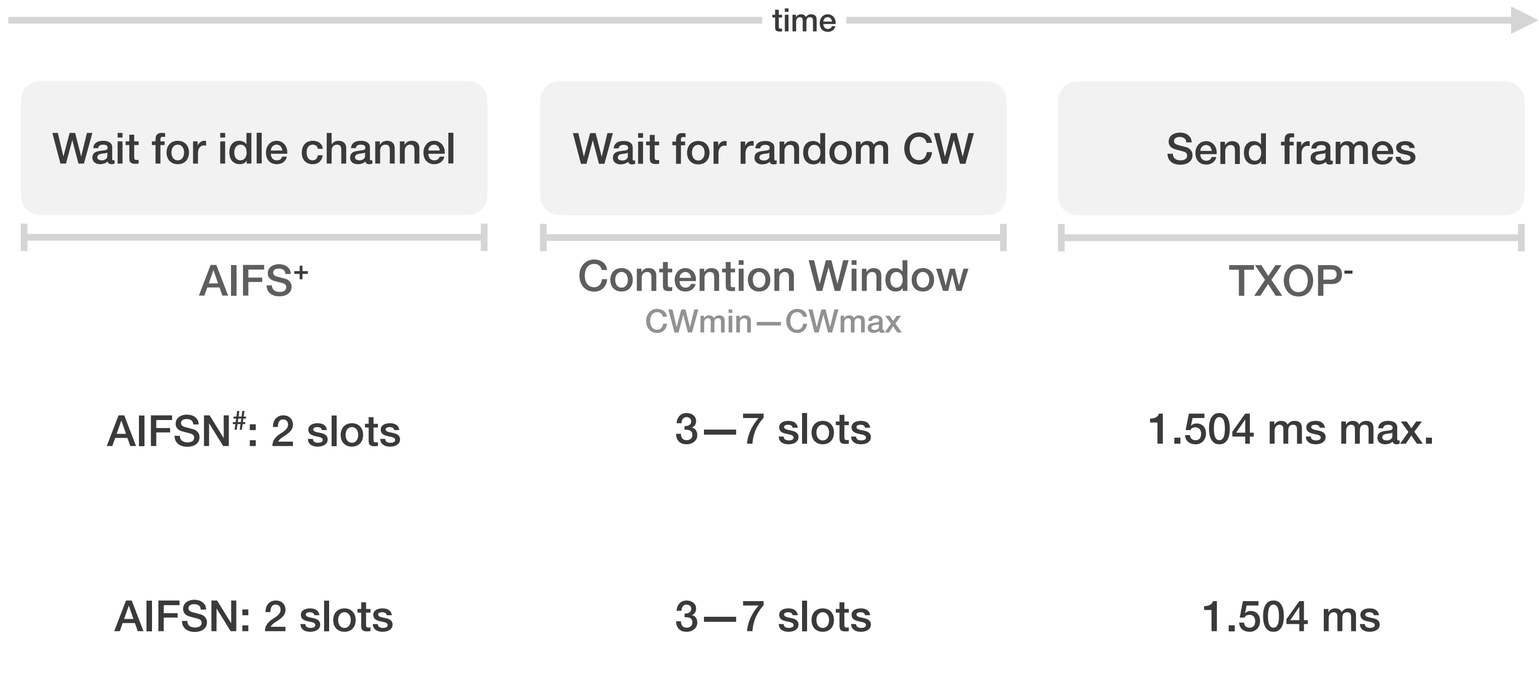
AIFSN: AIFS Number

TXOP: Transmission Opportunity

AIFS: Arbitration Inter-Fame Space

LLW Parameters

IEEE 802.11e Concepts



AIFSN: AIFS Number

TXOP: Transmission Opportunity

AIFS: Arbitration Inter-Fame Space

LLW Parameters

IEEE 802.11e Concepts

time

Parameters for Voice	Wait for idle channel AIFS[+]	Wait for random CW Contention Window CWmin—CWmax	Send frames TXOP[-]
IEEE 802.11-2012	AIFSN[#]: 2 slots	3—7 slots	1.504 ms max.
LLW `defaultVOLLWParams`	AIFSN: 2 slots	3—7 slots	1.504 ms
LLW `defaultLLWParams`	AIFSN: 2 slots	non-ETSI countries: 0—1 slots ETSI countries: 3—7 slots	non-ETSI countries: 8.160 ms (255 * 32 µs) ETSI countries: 1.984 ms (62 * 32 µs)

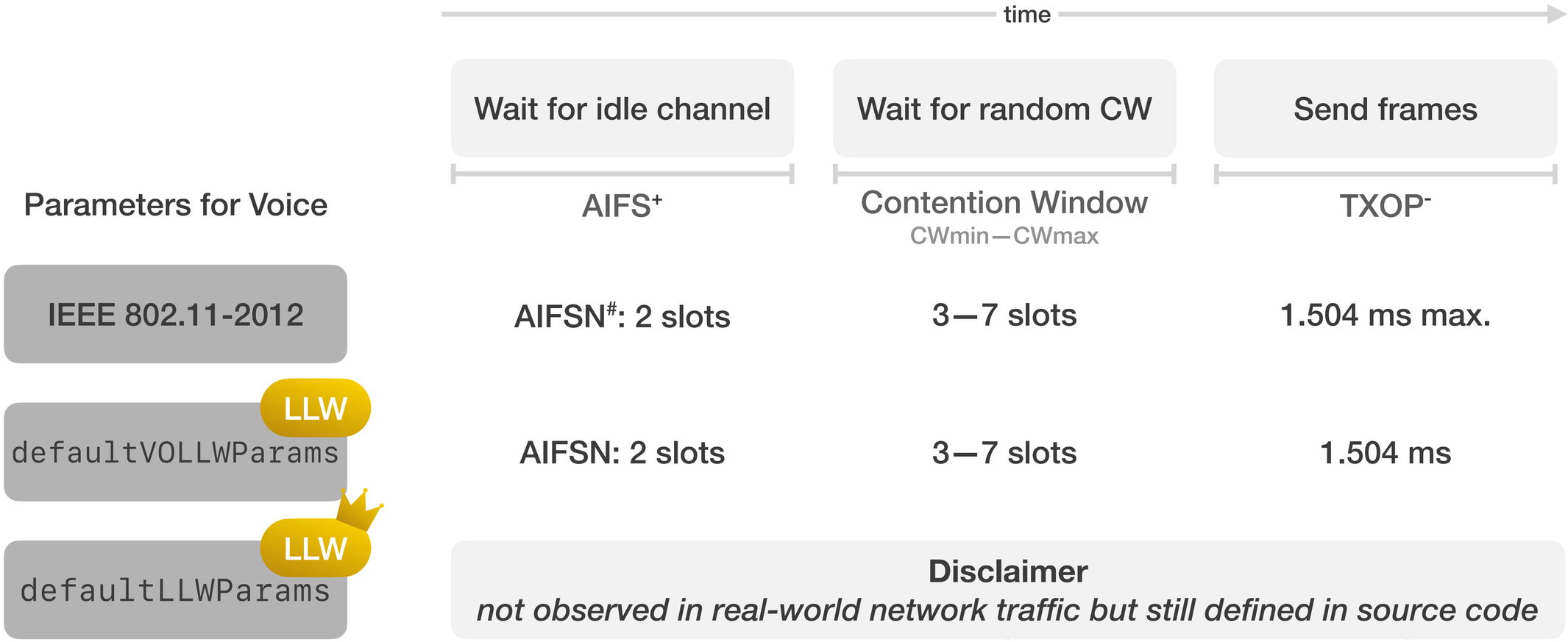
AIFSN: AIFS Number

− TXOP: Transmission Opportunity

+ AIFS: Arbitration Inter-Fame Space

LLW Parameters

IEEE 802.11e Concepts



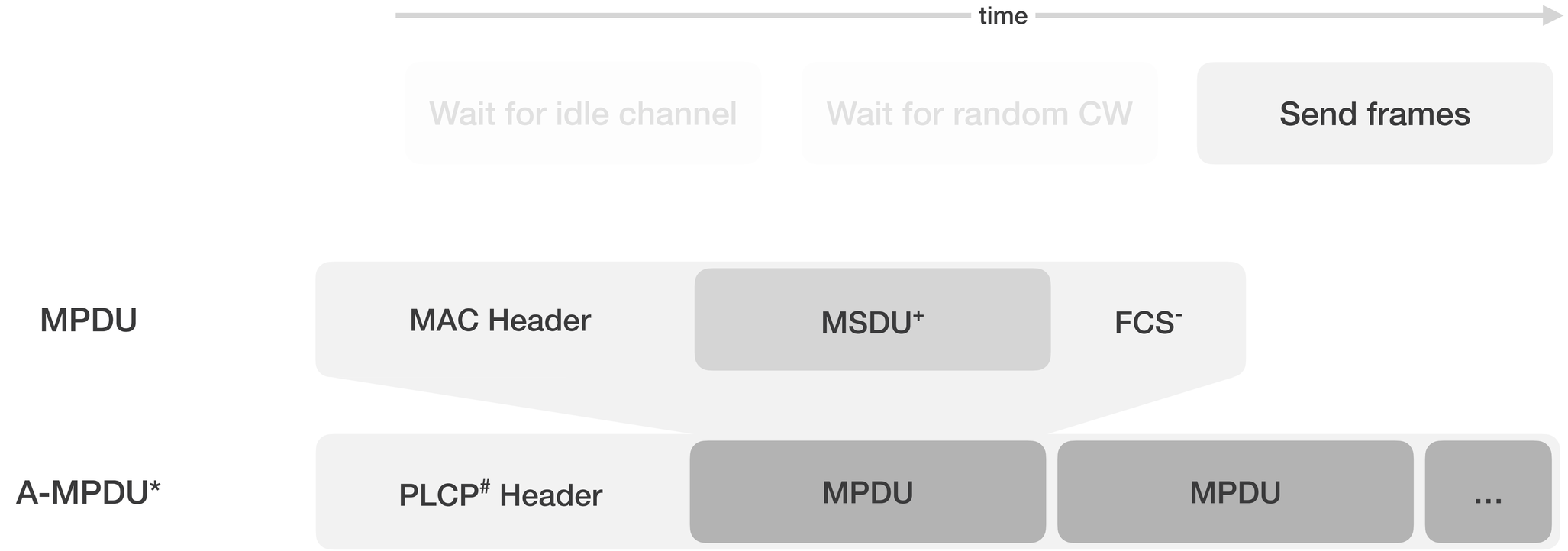
AIFSN: AIFS Number

TXOP: Transmission Opportunity

AIFS: Arbitration Inter-Fame Space

Aggregated MPDU

IEEE 802.11n Concepts



⊕ MSDU: MAC service data unit ⊖ FCS: Frame Check Sequence

✱ A-MPDU: Aggregated MAC Protocol Data Unit # PLCP: Physical Layer Convergence Protocol

[R]

Aggregated MSDU

IEEE 802.11n Concepts

Latency Gains

✅ Less IFS

✅ Less PHY headers, MAC headers, FCS

✅ Less acknowledgement frames

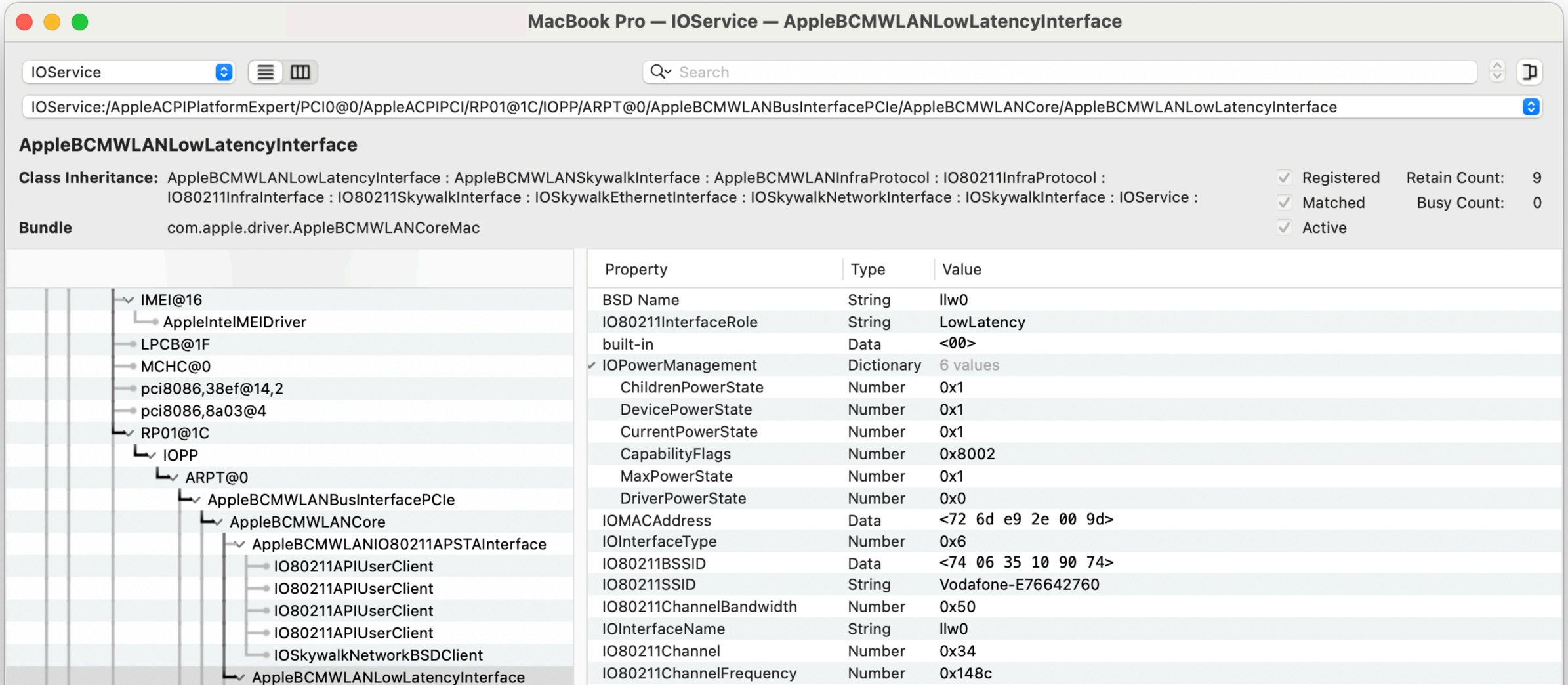
⊛ A-MSDU: Aggregated MAC Protocol Data Unit

⊖ FCS: Frame Check Sequence ⊕ MSDU: MAC service data unit

[R]

VHT Bandwidth

IEEE 802.11ac Concepts



VHT Bandwidth

IEEE 802.11ac Concepts

IO80211ChannelBandwidth	Number	0x50
IOInterfaceName	String	llw0
IO80211Channel	Number	0x34
IO80211ChannelFrequency	Number	0x148c
IOInterfaceUnit	Number	0x0
IOInterfaceNamePrefix	String	llw
IO80211Band	String	5 GHz

VHT Bandwidth

IEEE 802.11ac Concepts

IO80211ChannelBandwidth	Number	0x50
IOInterfaceName	String	llw0
IO80211Channel	Number	0x34
IO80211ChannelFrequency	Number	0x148c
IOInterfaceUnit	Number	0x0
IOInterfaceNamePrefix	String	llw
IO80211Band	String	5 GHz

→ 80 MHz Channel Bandwidth

↓

IEEE 802.11ac

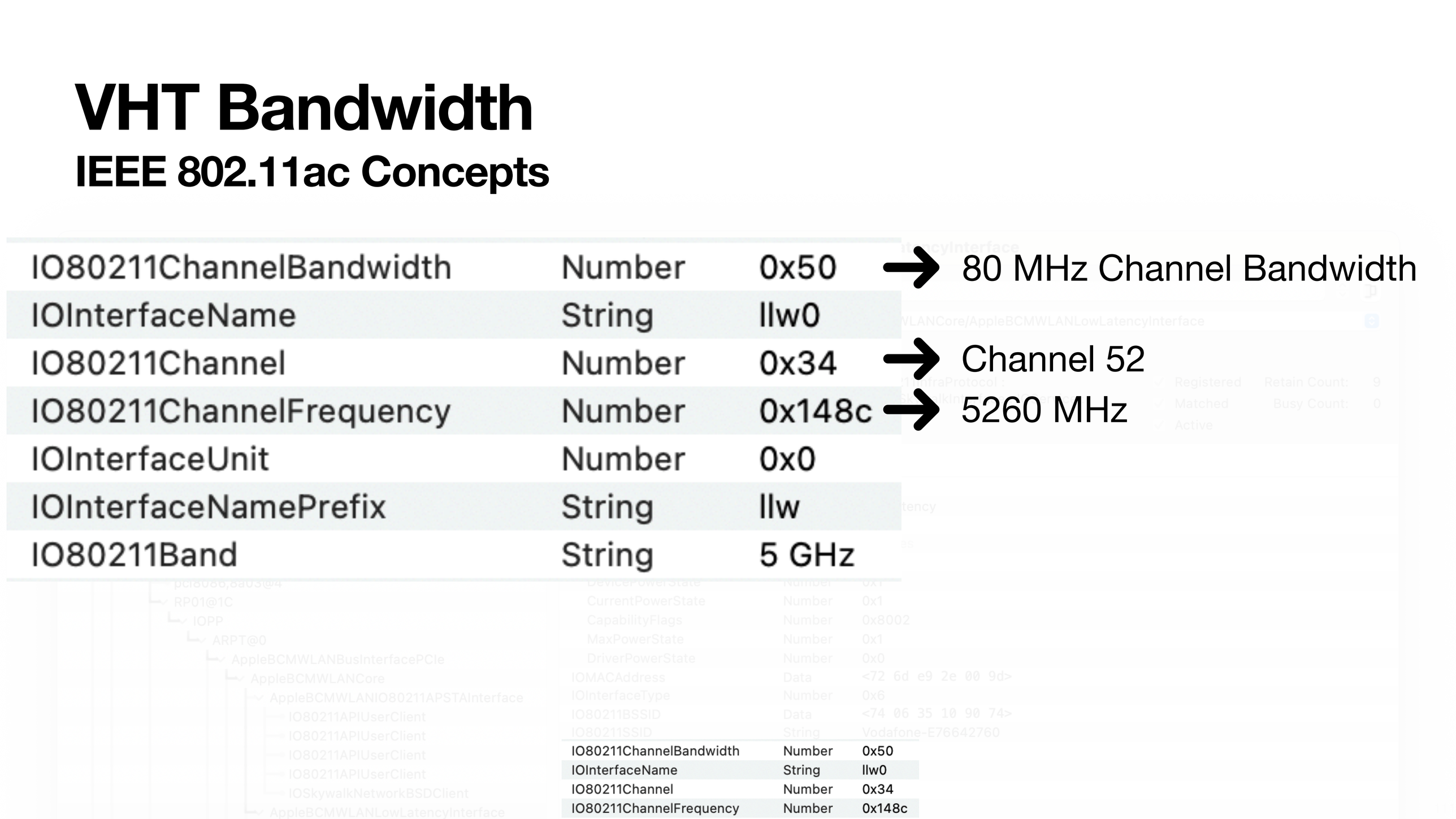
↓

Very High Throughput (VHT) PHY

VHT Bandwidth

IEEE 802.11ac Concepts

IO80211ChannelBandwidth	Number	0x50	→ 80 MHz Channel Bandwidth
IOInterfaceName	String	llw0	
IO80211Channel	Number	0x34	→ Channel 52
IO80211ChannelFrequency	Number	0x148c	→ 5260 MHz
IOInterfaceUnit	Number	0x0	
IOInterfaceNamePrefix	String	llw	
IO80211Band	String	5 GHz	



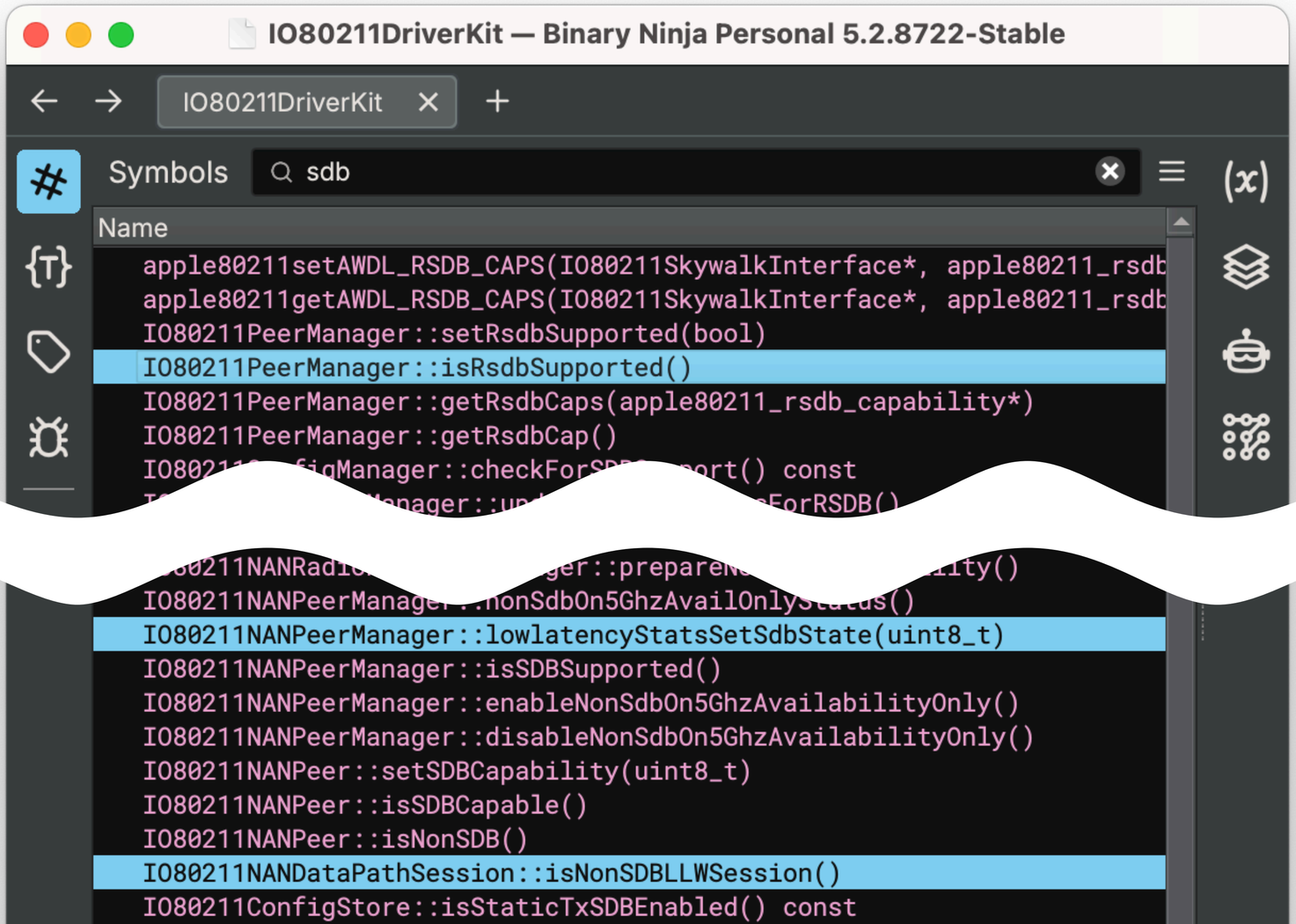
Low-Latency in LLW

IEEE 802.11e/n/ac Details

Hardware Capabilities

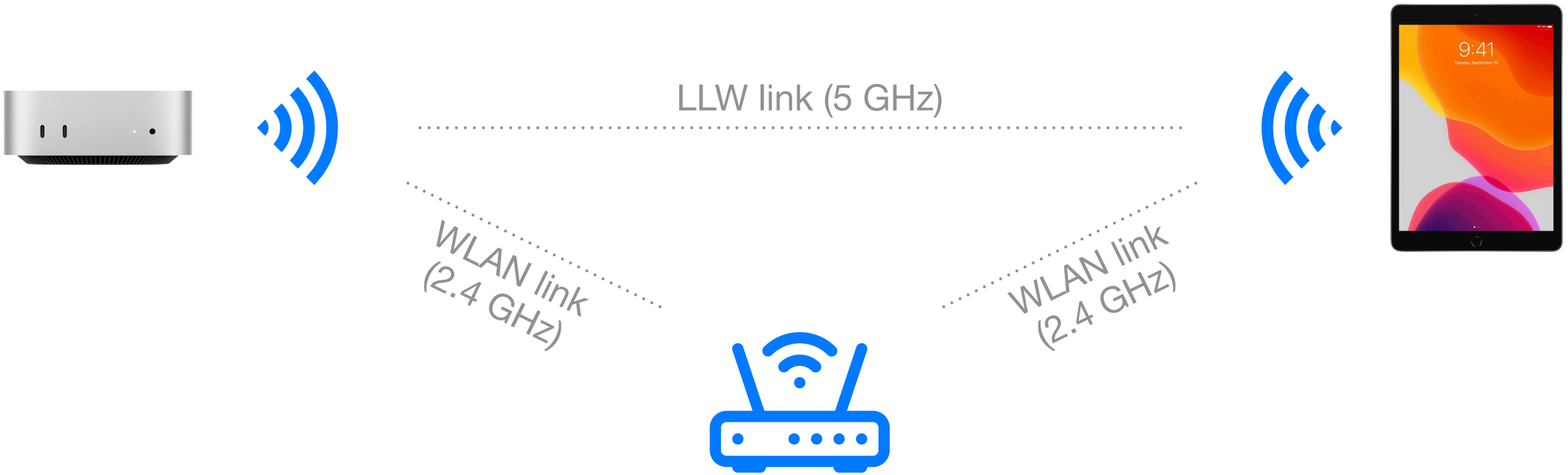
Real Simultaneous Dual Band (RSDB)

Hardware Capabilities



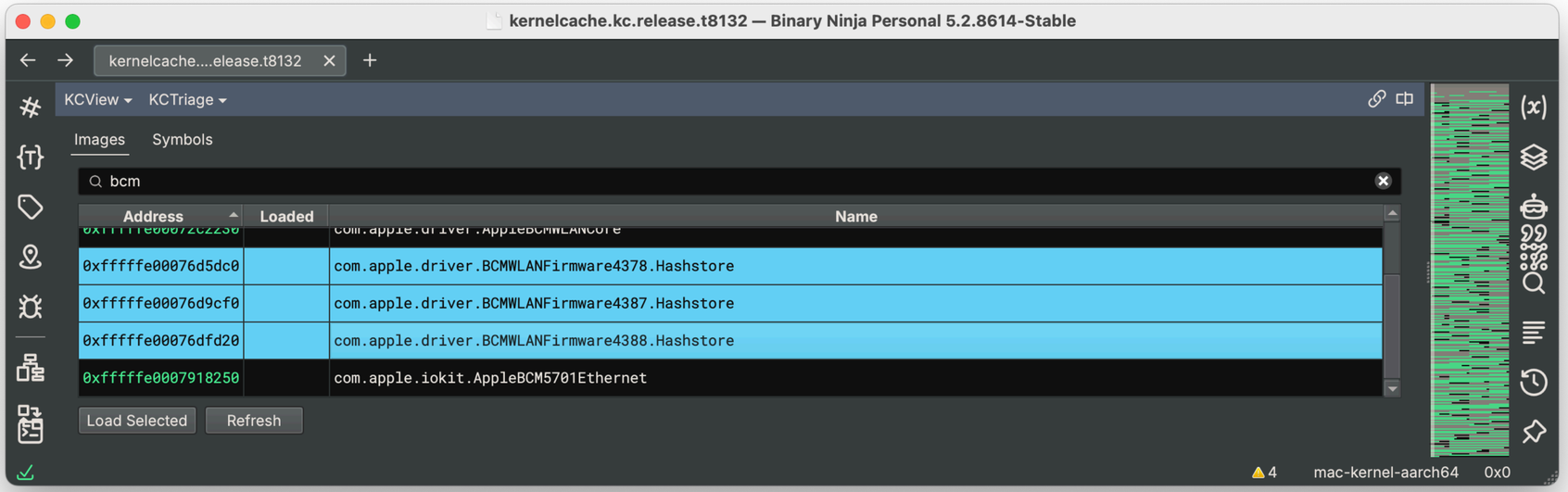
Real Simultaneous Dual Band (RSDB)

Hardware Capabilities



Real Simultaneous Dual Band (RSDB)

Hardware Capabilities



BCM4378	PCIe 2.0 / SDIO 3.0	abgn+ac+ax	2x2:2 (1.43Gbps)	2019-02-06	Combo BT 5.0 LE/LR, RSDB, OFDMA, **Wi-Fi 6, MU-MIMO, HE80, 1024QAM** Smartphone Combo Chip	1 devices	0 devices	PR PR CNX PPage
BCM4387	PCIe 2.0 / SDIO 3.0	abgn+ac+ax	2x2:2 (2.4Gbps)	(Q2 2020)	Combo BT 5.2 LE/LR, RSDB, OFDMA, **Wi-Fi 6, MU-MIMO, HE160, 1024QAM** **WPA3+, TBS, 5GHz**, mobile devices	0 devices	0 devices	PR PPage DR
BCM4388	PCIe 2.0 / SDIO 3.0	abgn+ac+ax	2x2:2 (2.4Gbps)	(Q2 2022)	Combo BT 5.3 LE/LR, RSDB, OFDMA, **Wi-Fi 6E, MU-MIMO, HE160, 1024QAM** **WPA3+, TBS, 6GHz**, mobile devices	0 devices	0 devices	PR PPage DR

Real Simultaneous Dual Band (RSDB)

Hardware Capabilities

BCM4375	PCIe 2.0 / SDIO 3.0	abgn+ac+ax	2x2:2 (1.43Gbps)	2019-02-15	Combo BT 5.0 LE/LR, RSDB, OFDMA, **Wi-Fi 6, MU-MIMO, HE80, 1024QAM** Smartphone Combo Chip	0 devices	1 devices	PR PR CNX PPage

	Type	FCC ID	Manuf	Manuf. mdl	CPU1	CPU1 clock speed	FLA1	RAM1	WI1 chip1	PHY modes	OUI	OUI (Eth)	Est. year
Samsung Galaxy S10 (SM-G973U)		A3LSMG973U A3LSMG975U A3LSMG970U	Samsung		SM8150	2.84 GHz	524,288 MiB	8,192 MiB	BCM4375	abgn+ac+ax	00:12:36		2019

Access Category

Voice

Access Control Mandatory Frame Reordering

NAV MAC-Layer Efficiency Threshold

Block Acknowledgements Reverse Direction Grant

80 MHz
Channel Bandwidth

Ultra
LLW

Real-time
LLW

More Operational Modes

Low-Latency Mechanisms of Low-Latency WiFi

Aggregated MSDU | Aggregated MPDU

Frame Overhead Reduction

IEEE 802.11e/n/ac

QoS | HT | VHT

1.504 ms TXOP | Long Transmission Intervals

3 slots CWmin | 7 slots CWmax | 2 slots AIFSN

Fast Channel Access

Traffic Identifier 7

High-Priority Network Traffic

Why bother?

Interoperability.

Apple is implementing an open standard but leaves LLW undocumented and reserves it for proprietary features.

Interoperability is technically feasible.

OpenDrop

WatchWitch

OpenHaystack

Pending?

[23] [24] [25] [AD] [AE] [AF]

python-pcapng

cctool

IEEE 802.11e

Log Aggregation

Real Simultaneous Dual-Band

Inter-Frame Space

Interoperability

DriverKit

Access Categories

A-MSDU

Questions?

NTP

System Calls

kdebug

TXOP

dtrace

Multi-Device Log Acquisition

Low-Latency WiFi

IEEE 802.11n

Contention Window

Kernel Traces

_driverkit user

henri.jaeger@uni-potsdam.de

Special thanks to jiska.

Literature

[A] Inga Susanna Dischinger. Security Analysis of Apple’s Continuity Camera for iPhone. Technische Universität Darmstadt, October 30, 2023

[B] Jan Dominik Röper. Sicherheitsanalyse von Apple’s Sidecar-Protokoll. Technische Universität Darmstadt, August 02, 2023

[C] https://support.apple.com/en-us/108046 (visited 09/12/2025)

[D] https://www.openkritis.de/ (visited 17/12/2025)

[E] https://developer.apple.com/bug-reporting/profiles-and-logs/ (visited 17/12/2025)

[F] David Kreitschmann. User manual for the Apple CoreCapture Framework. July 17, 2018. URL: https://arxiv.org/abs/1808.07353 (visited on 09/12/2025)

[G] https://discord.gg/NAxRYvysuc (visited on 17/12/2025)

[H] https://github.com/apple-oss-distributions/system_cmds (visited on 17/12/2025)

[I] https://github.com/apple-oss-distributions/system_cmds/releases/tag/system_cmds-918.100.3 (visited on 17/12/2025)

Literature

[J] https://github.com/apple-oss-distributions/system_cmds/tree/559f661c5687f7828307cb3b1026a45f849243c6 (visited on 17/12/2025)

[K] https://github.com/apple-oss-distributions/system_cmds/tree/559f661c5687f7828307cb3b1026a45f849243c6/trace.tproj (visited on 17/12/2025)

[L] https://datatracker.ietf.org/doc/rfc5905 (visited on 09/12/2025)

[M] https://developer.apple.com/download/all/?q=Kernel%20Debug%20Kit (visited on 09/12/2025)

[N] https://download.developer.apple.com/macOS/Kernel_Debug_Kit_15.2_build_24C101/Kernel_Debug_Kit_15.2_build_24C101.dmg (visited on 17/12/2025)

[O] https://github.com/jprx/PacmanPatcher/blob/main/README.md#booting-the-patched-kernel (visited on 17/12/2025)

[P] https://gist.github.com/steven-michaud/fda019a4ae2df3a9295409053a53a65c (visited on 17/12/2025)

Literature

[Q] IEEE Computer Society. IEEE Standard for Information technology–Local and metropolitan area networks–Specific requirements–Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications - Amendment 8: Medium Access Control (MAC) Quality of Service Enhancements. IEEE Std 802.11e-2005 (Amendment to IEEE Std 802.11, 1999 Edition (Reaff 2003) (Nov. 11, 2005), 1–212. URL: https://ieeexplore.ieee.org/document/1541572 (visited on 09/12/2025)

Literature

[R] IEEE Computer Society. IEEE Standard for Information technology– Local and metropolitan area networks–Specific requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 5: Enhancements for Higher Throughput. IEEE Std 802.11n-2009 (Amendment to IEEE Std 802.11-2007 as amended by IEEE Std 802.11k-2008, IEEE Std 802.11r-2008, IEEE Std 802.11y-2008, and IEEE Std 802.11w-2009) (Oct. 29, 2009), 1–565. URL: https://ieeexplore.ieee.org/document/5307322 (visited on 09/12/2025)

[S] Eldad Perahia and Robert Stacey. Next Generation Wireless LANs: Through- put, Robustness, and Reliability in 802.11n. 1st ed. Cambridge University Press, 2008. URL: https://www.cambridge.org/core/books/next-generation-wireless-lans/878A3498E9966D24E9B47B47B454094A (visited on 09/12/2025)

[T] https://dot11ap.wordpress.com/edca-channel-access-method (visited on 09/12/2025)

Literature

[U] IEEE Computer Society. IEEE Standard for Information Technology–Telecommunications and Information Exchange between Systems Local and Metropolitan Area Networks–Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. IEEE Std 802.11-2024 (Revision of IEEE Std 802.11-2020) (Apr. 28, 2025), 1–5956. URL: https://ieeexplore.ieee.org/document/10979691 (visited on 09/12/2025)

Literature

[V] IEEE Computer Society. IEEE Standard for Information technology–Telecommunications and information exchange between systems Local and metropolitan area networks–Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. IEEE Std 802.11-2012 (Revision of IEEE Std 802.11-2007) (Mar. 29, 2012), 1–2793. URL: https://ieeexplore.ieee.org/document/6178212 (visited on 17/12/2025)

[W] IEEE Computer Society. IEEE Standard for Information technology–Telecommunications and information exchange between systems—Local and metropolitan area networks–Specific requirements–Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications–Amendment 4: Enhancements for Very High Throughput for Operation in Bands below 6 GHz (Dec. 18, 2013). URL: https://ieeexplore.ieee.org/document/7797535 (visited on 17/12/2025)

Literature

[X] https://patentimages.storage.googleapis.com/45/4a/11/ceadc6d8a02596/US9019898.pdf (visited on 09/12/2025)

[Y] WikiDevi.Wi-Cat.RU. Broadcom. WikiDevi.Wi-Cat.RU. July 27, 2023. URL: https://wikidevi.wi-cat.ru/Broadcom (visited on 09/12/2025)

[Z] https://wikidevi.wi-cat.ru/index.php/Special:Ask?title=Special%3AAsk&q=%3Cq%3E%3Cq%3E%5B%5BWI1+chip1+model::BCM4375%5D%5D+%5B%5BWI1+chip1+model::!~BCM4375X*%5D%5D%3C%2Fq%3E+OR+%3Cq%3E%5B%5BWI2+chip1+model::BCM4375%5D%5D+%5B%5BWI2+chip1+model::!~BCM4375X*%5D%5D%3C%2Fq%3E%3C%2Fq%3E&po=%3FEmbedded+system+type=Type%0D%0A%3FFCC+ID%0D%0A%3FManuf%0D%0A%3FManuf+product+model=Manuf.+mdl%0D%0A%3FCPU1+model=CPU1%0D%0A%3FCPU1+clock+speed%0D%0A%3FFLA1+amount=FLA1%0D%0A%3FRAM1+amount=RAM1%0D%0A%3FWI1+chip1+model=WI1+chip1%0D%0A%3FSupported+802dot11+protocols=PHY+modes%0D%0A%3FOUI%0D%0A%3FOUI+(ethernet)=OUI+(Eth)%0D%0A%3FEstimated+year+of+release=Est.+year&eq=yes&p%5Bformat%5D=broadtable&order%5B0%5D=ASC&sort_num=&order_num=ASC&p%5Blimit%5D=500&p%5Boffset%5D=&p%5Blink%5D=all&p%5Bsort%5D=&p%5Bheaders%5D=show&p%5Bmainlabel%5D=&p%5Bintro%5D=&p%5Boutro%5D=&p%5Bsearchlabel%5D=…+further+results&p%5Bdefault%5D=&p%5Bclass%5D=sortable+wikitable+smwtable (visited on 15/12/2025)

Literature

[AA] Kamesh Medepalli. CYW89459: High Performance and Low Power Wi-Fi and Bluetooth 5.1 Combo Chip for IoT and Automotive. In: 2019 IEEE Hot Chips 31 Symposium (HCS). 2019 IEEE Hot Chips 31 Symposium (HCS). Cupertino, CA, USA: IEEE, Aug. 2019, 1–18. isbn: 978-1-7281-2089-8. URL: https://ieeexplore.ieee.org/document/8875681/ (visited on 09/12/2025)

[AB] Shing Tak Yan, Lu Ye, Hongbing Wu, Raghavendra Kulkarni, Edward Myers, Hsieh-Chih Shih, Shadi Saberi, Darshan Kadia, Dizle Ozis, Lei Zhou, Eric Mid- dleton, and Joo Leong Tham. An 802.11a/b/g/n/ac WLAN Transceiver for 2 × 2 MIMO and simultaneous dual-band operation with +29 dBm Psat integrated power amplifiers. In: ESSCIRC Conference 2016: 42nd European Solid-State Circuits Conference. ESSCIRC Conference 2016: 42nd European Solid-State Circuits Conference. Sept. 2016, 121–124. URL: https://ieeexplore.ieee.org/document/7598257/ (visited on 17/12/2025)

[AC] IEEE Computer Society. IEEE Standard for Local and metropolitan area networks: Media Access Control (MAC) Bridges. IEEE Std 802.1D-2004 (Revision of IEEE Std 802.1D-1998) (June 9, 2004), 1–281. URL: https://ieeexplore.ieee.org/document/1309630/(visited on 09/12/2025)

Literature

[AD] https://github.com/seemoo-lab/opendrop (visited on 09/12/2025)

[AE] https://github.com/seemoo-lab/watchwitch (visited on 09/12/2025)

[AF] https://github.com/seemoo-lab/openhaystack (visited on 09/12/2025)

Figures

[1] https://store.storeimages.cdn-apple.com/1/as-images.apple.com/is/studio-display-gallery-1-202203?wid=640&hei=528&fmt=p-jpg&qlt=95 (visited on 09/12/2025)

[2] https://store.storeimages.cdn-apple.com/1/as-images.apple.com/is/mac-mini-select-202410?wid=904&hei=840&fmt=jpeg&qlt=90&.v=WG0zcWo4VEd2YnZ3WTlBVlBwSHNCUnZ0SFlldzZrSzBMWjRQMnF1U2Y2enZhWUNqTDdqTGdxV2EvMEFJcW1vNDg0SERaYTF4eEZ1aW9ZbGpONkszSXRhaHNubVVXOWRtVW4zMGQxeFF6U00 (visited on 09/12/2025)

[3] https://upload.wikimedia.org/wikipedia/commons/thumb/d/d2/IPad_10.2-inch.png/1280px-IPad_10.2-inch.png (visited on 09/12/2025)

[4] https://cdsassets.apple.com/live/SZLF0YNV/images/sp/111911_sp807-ipad-7th-gen.png (visited on 09/12/2025)

Figures

[5] https://drive.google.com/file/d/1QvLTWECNhQpd10IlW1nz8nUTKvFup_jk/view (visited on 09/12/2025)

[6] https://store.storeimages.cdn-apple.com/1/as-images.apple.com/is/MXK53_AV1?wid=1144&hei=1144&fmt=jpeg&qlt=90&.v=QytENXB3MzdYRFA4RU1McS9kQ1d6VlZya2lKWlJmUEwrYndWOTJiVWJWQUYwVmtlbGRkS25RMVpBRlo0bk5DUStteWFnS2JDbkxFb1JqRG5KS1RPUWc (visited on 09/12/2025)

[7] https://store.storeimages.cdn-apple.com/1/as-images.apple.com/is/MXCL3D?wid=1144&hei=1144&fmt=jpeg&qlt=90&.v=MWhTMGgwN3h3cm1YQ0hHelVYWWZ2RExJNzJtbW9WRzBUckZ4SDR0aldyMFY0ZGtxRm5nMGhUUUYyQ1NONFVVUnBSYmQxNkhWTGV4d1BxVjd4aUJPSGc (visited on 09/12/2025)

[8] https://www.figma.com/community/file/1515522710546098726 (visited on 09/12/2025)

[9] https://cdsassets.apple.com/live/7WUAS350/images/macos/ventura/macos-ventura-macbook-pro-iphone-13-pro-continuity-camera-desk-view-hero.png (visited on 17/12/2025)

Figures

[10] https://istore.co.na/cdn/shop/files/iPhone_15_Pro_White_Titanium_PDP_Image_Position-8__WWEN_76d79726-ff49-4320-ab7b-316723a4ab0d_5000x.jpg?v=1707992983 (visited 17/12/2025)

[11] https://web.archive.org/web/20240917165129im_/https://cdsassets.apple.com/live/7WUAS350/images/macos/sequoia/macbook-air-13in-iphone-15-pro-macos-sequoia-ios-18-iphone-mirroring-hero.png (visited 17/12/2025)

[12] https://upload.wikimedia.org/wikipedia/commons/thumb/f/f2/Hasso-Plattner-Institut_logo.svg/1599px-Hasso-Plattner-Institut_logo.svg.png (visited on 17/12/2025)

[13] https://tenor.com/en-GB/view/huh-gif-5919216761975506496 (visited on 17/12/2025)

[14] https://de.wikipedia.org/wiki/Python_(Programmiersprache)#/media/Datei:Python-logo-notext.svg (visited on 17/12/2025)

[15] https://en.wikipedia.org/wiki/Ghidra#/media/File:Ghidra_logo.svg (visited on 17/12/2025)

Figures

[16] https://www.kotsovolos.gr/computing/laptop-tablet-ipad/notebook-macbook-ultrabook/212066-apple-macbook-pro-13-2020-touch-bar-4-core-i5-20ghz-8gb-1tb-space-grey?srsltid=AfmBOoqFw1TlJlf96x7qjNdUsLpjROnsxmUVjYRrqbkhdbLC1oIVqeDF (visited on 09/12/2025)

[17] https://store.storeimages.cdn-apple.com/1/as-images.apple.com/is/MMEL2?wid=1144&hei=1144&fmt=jpeg&qlt=95&.v=aXR3b2ZFdWtrcnZKeHJPL012ZjgxUWtuVHYzMERCZURia3c5SzJFOTlPaWI2elFubVhUMUdUbUxPYVZ3Z2lNVkdQRGIwQWs0TnlIc0d0NVF0QUNPMXc (visited on 09/12/2025)

[18] https://procare.gr/en/mac-cables-adapters/405-apple-thunderbolt-to-gigabit-ethernet-adapter-885909561247.html (visited on 09/12/2025)

[19] https://www.123ink.gr/123inkt-Kalodio-diktyou-123ink-Cat6a-U-UTP-nkri-5-metra-21990875C-55423C-K8109GR-5C-i102143-t2270236.html?utm_source=google&utm_medium=cpc&utm_campaign=PPC-SEA-GR-Google-Shopping-B-Office-Other-Types&gad_source=1&gad_campaignid=23160965674&gbraid=0AAAAAqK-a5m1OVql5inwtDpVfZGxS5C_I&gclid=EAIaIQobChMIgOjM9KShkQMVQPJ5BB2HpwGNEAQYByABEgIIefD_BwE (visited on 09/12/2025)

Figures

[20] https://imgflip.com/memegenerator/236504287/Incredulous (visited on 17/12/2025)

[21] https://img.freepik.com/free-photo/grunge-wall-texture_1194-6371.jpg?t=st=1764838379~exp=1764841979~hmac=9cbca8804f3cd7de594b4b763122a01b62f23463ffc73b72ead16e1a0ce18e63&w=2000 (visited on 09/12/2025)

[22] https://upload.wikimedia.org/wikipedia/commons/thumb/1/17/AirPlay_2_logo.svg/1024px-AirPlay_2_logo.svg.png (visited on 09/12/2025)

[23] https://web.archive.org/web/20250904210947/https://de.wikipedia.org/wiki/AirDrop#/media/Datei:AirDrop_logo.svg (visited on 09/12/2025)

[24] https://www.apple.com/newsroom/images/live-action/wwdc-2023/standard/watchos-10/Apple-WWDC23-watchOS-10-new-Watch-faces-Palette-Iris-230605_inline.jpg.large.jpg (visited on 09/12/2025)

[25] https://en.wikipedia.org/wiki/Find_My#/media/File:Find_My_logo.svg (visited on 09/12/2025)