

Trespassing the Walled Garden

Teaching Linux to Speak Apple's Low-Latency WiFi

Henri Jäger-Menn

whoami

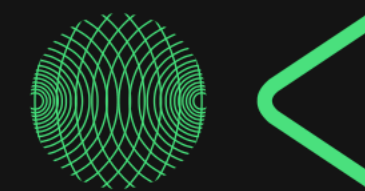
PhD Student @ Hasso Plattner Institute

Mobile and Wireless Security



Fellow 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.

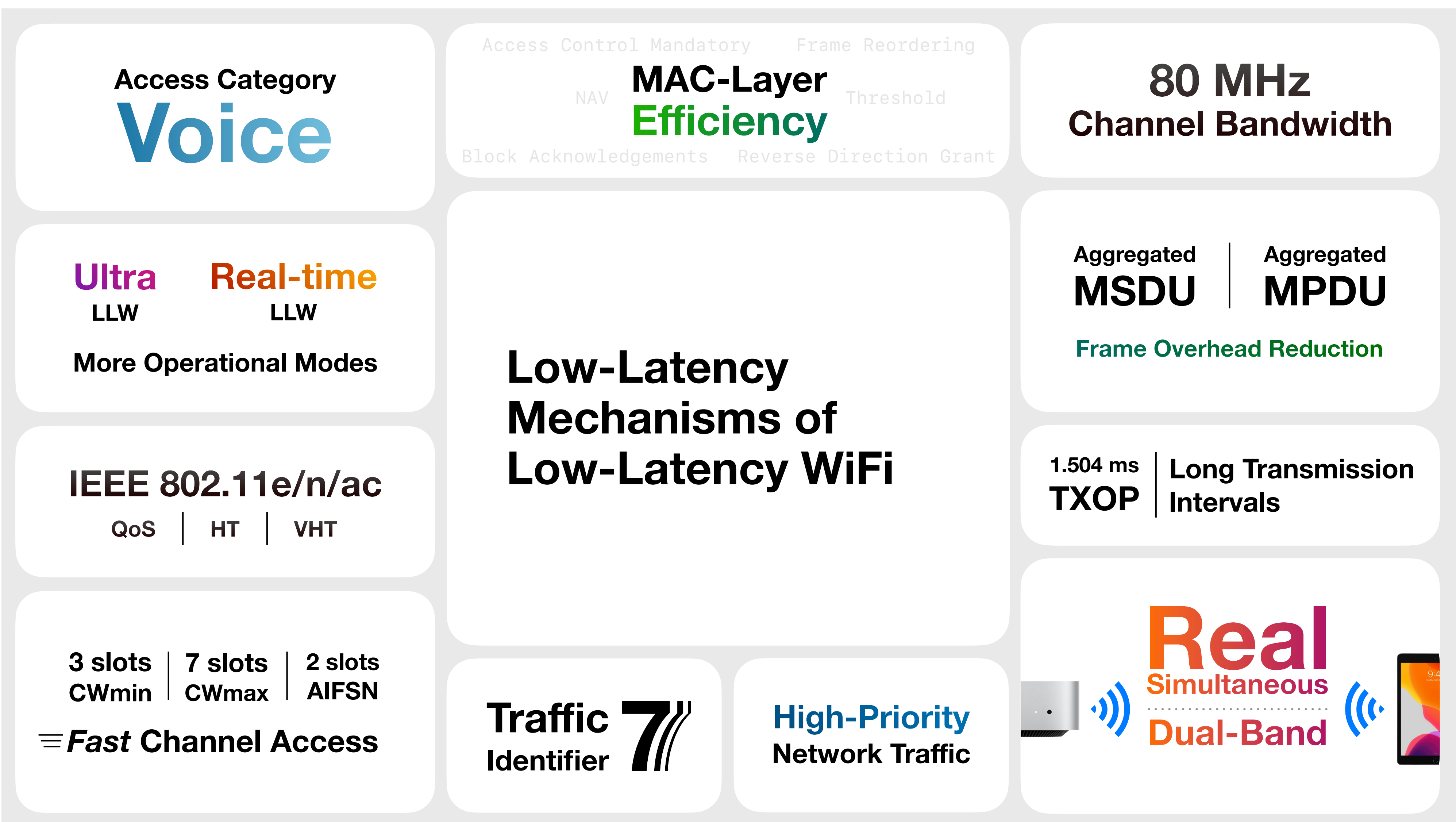


KRITIS und NIS2

[A]



Kritische Infrastrukturen



39C3, December 2025

How do we bring this to open platforms?

Recap: Low-Latency WiFi





Sidecar Display





Universal Control





Continuity Camera





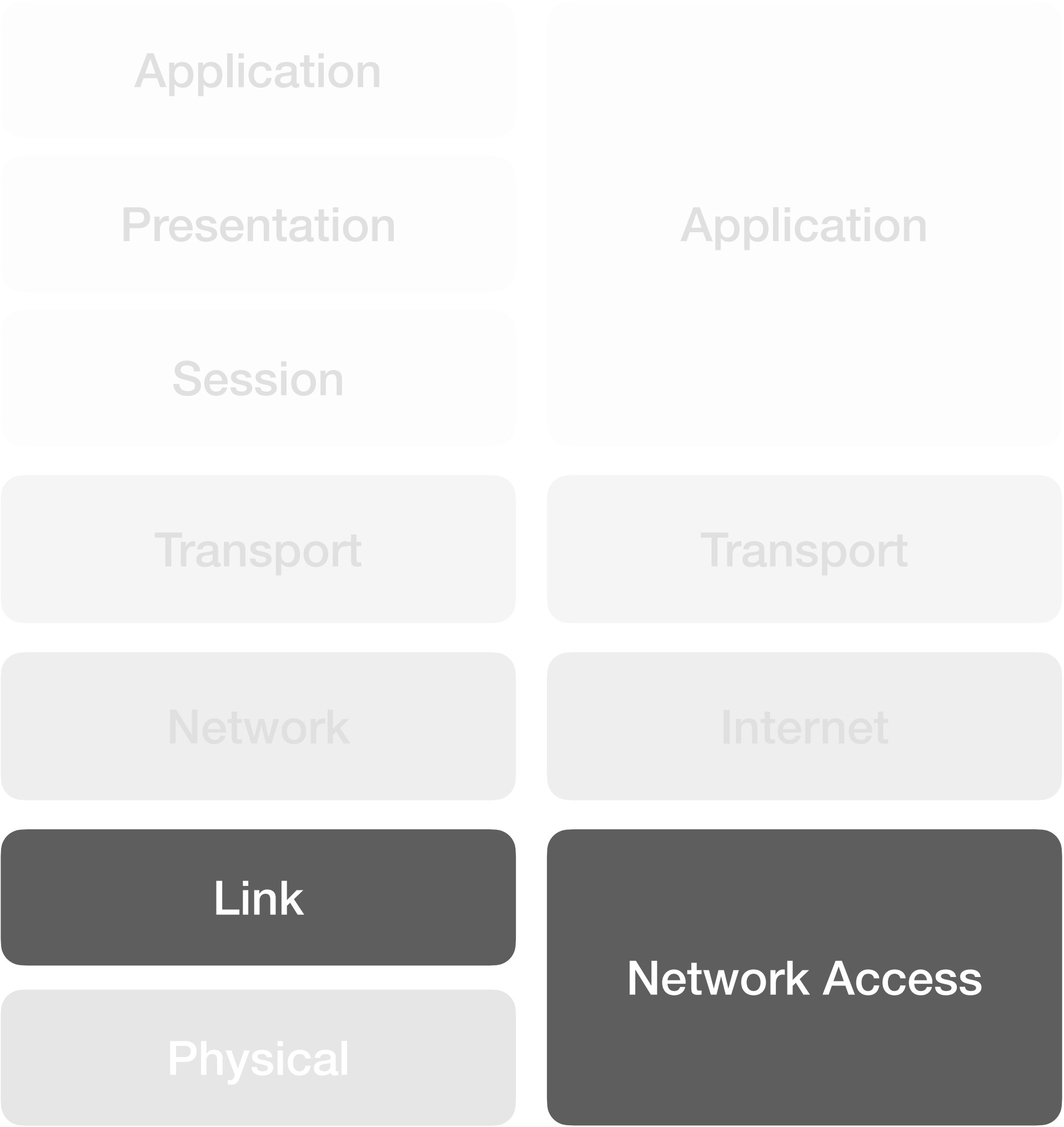
iPhone Mirroring



Mostly Video Data

Real-Time Constraints

Low-Latency WiFi ✨



Sidecar Display
Continuity Camera
iPhone Mirroring

UDP

IPv6

LLW

Low-Latency in LLW

IEEE 802.11e/n/ac

Hardware Capabilities

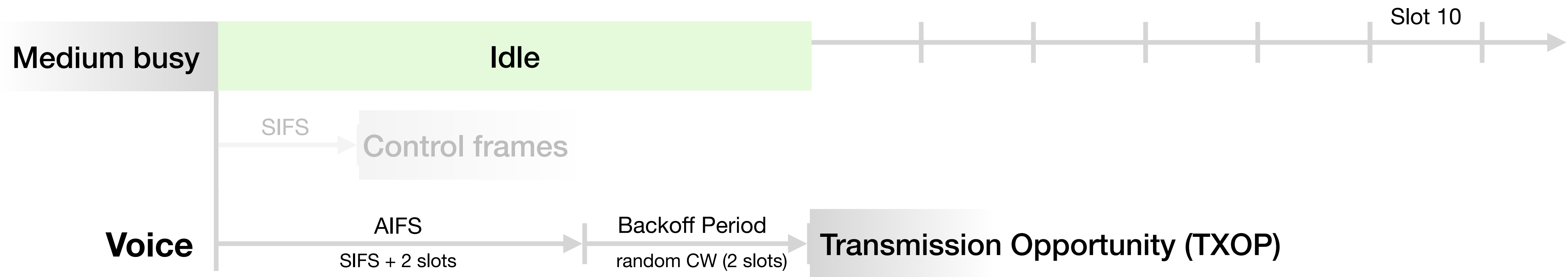
Enhanced Distributed Channel Access

IEEE 802.11e Concepts



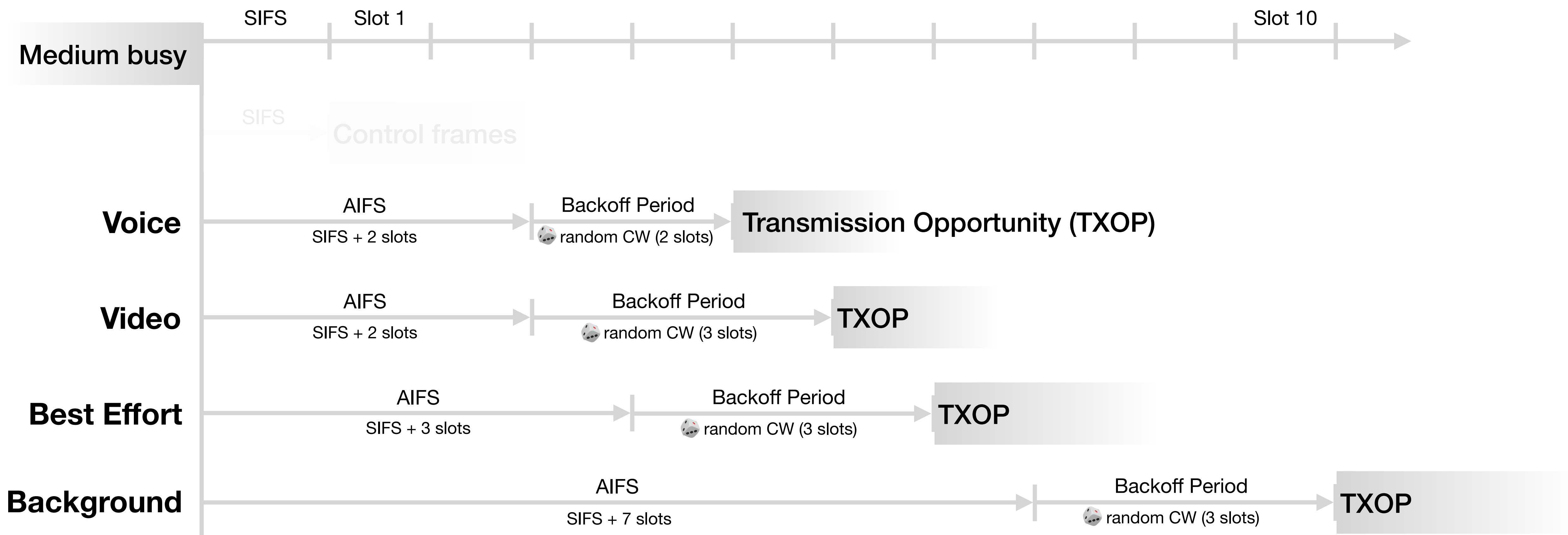
Enhanced Distributed Channel Access

IEEE 802.11e Concepts



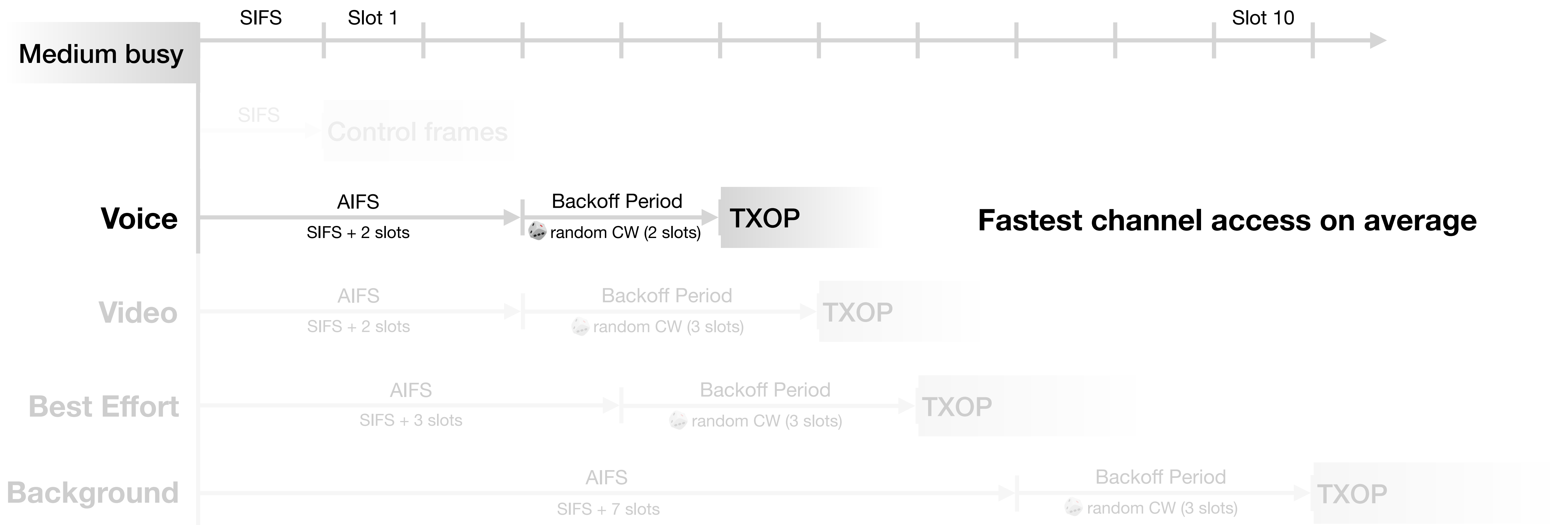
Enhanced Distributed Channel Access

IEEE 802.11e Concepts



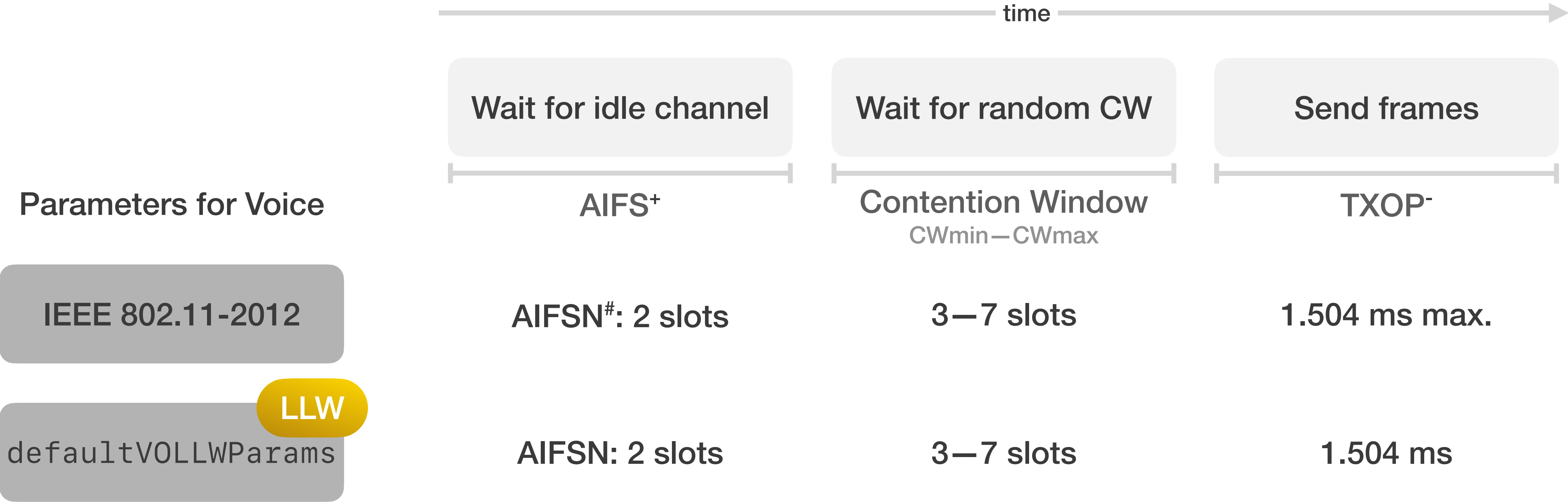
Enhanced Distributed Channel Access

IEEE 802.11e Concepts



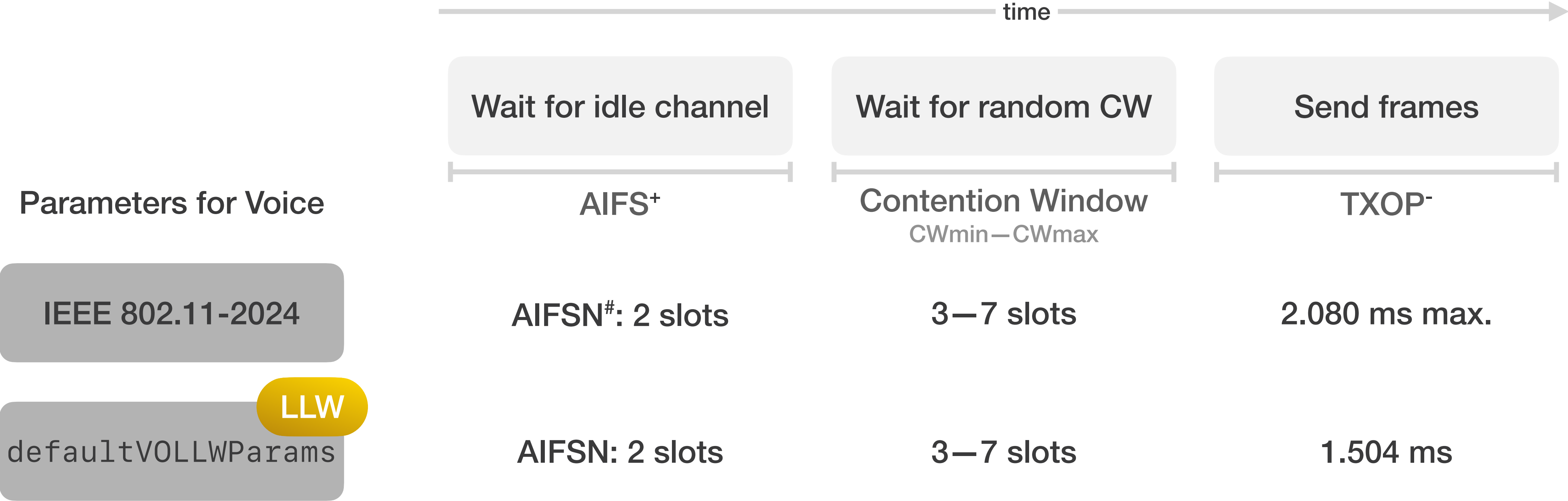
LLW Parameters

IEEE 802.11e Concepts



LLW Parameters

IEEE 802.11e Concepts



IEEE 802.11e

Quality of Service

Enhanced **D**istributed **C**hannel **A**ccess
Access Categories
Arbitration Inter-**F**rame **S**pacing
Contention **W**indow (max, min)
Transmission Opportunity (**T**XOP)
Block Acknowledgement

IEEE 802.11n

High Throughput

Aggregated **M**SDU
Aggregated **M**PDU
Reverse **D**irection Grant

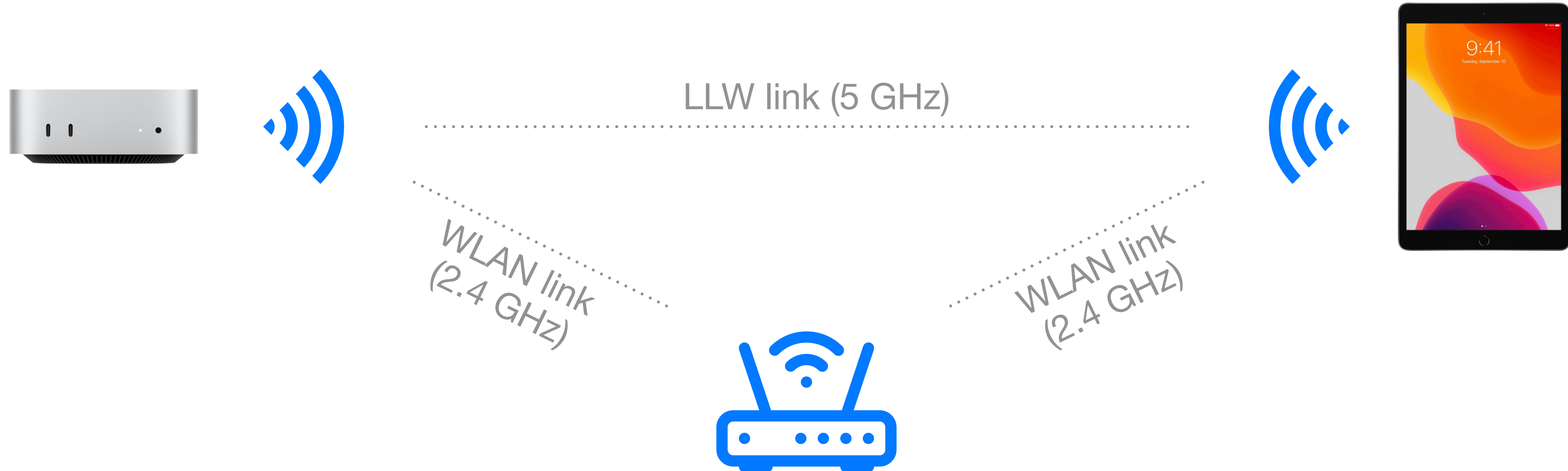
Low-Latency in LLW

IEEE 802.11e/n/ac

Hardware Capabilities

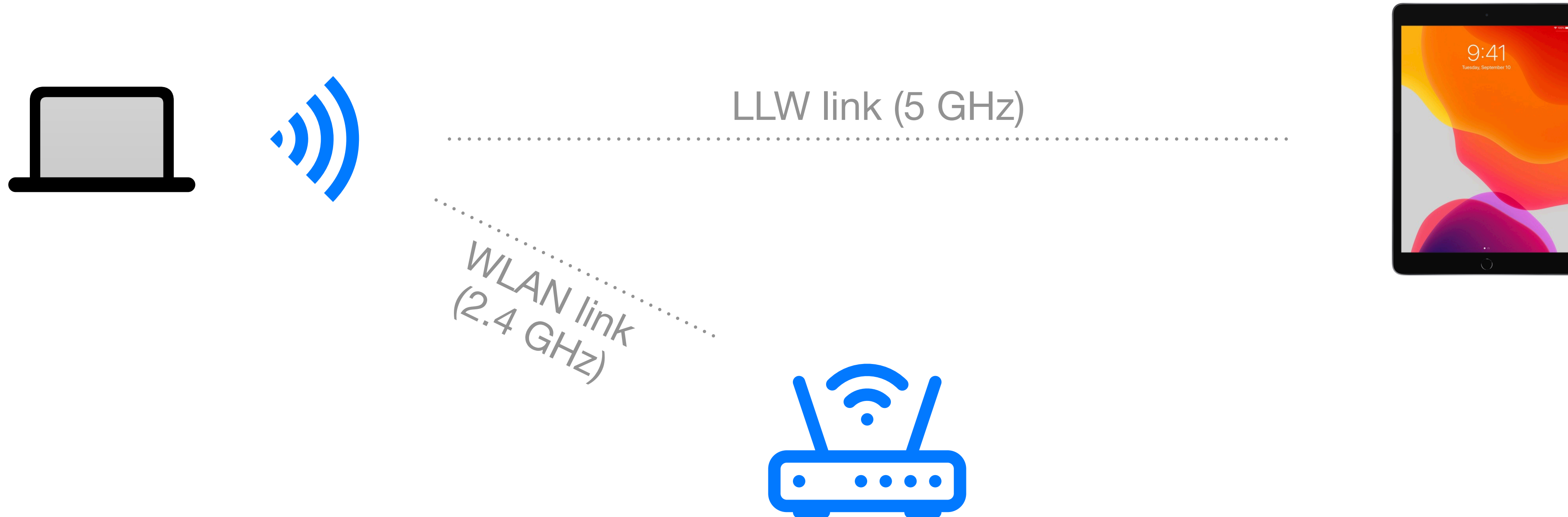
Real Simultaneous Dual Band (RSDB)

Hardware Capabilities



Real Simultaneous Dual Band (RSDB)

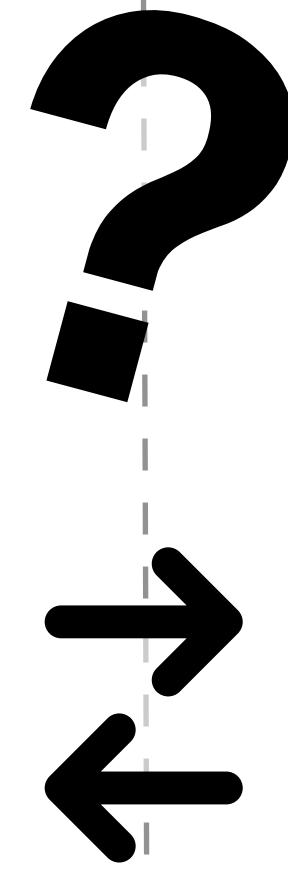
Hardware Capabilities



Identifying **trace points** on macOS

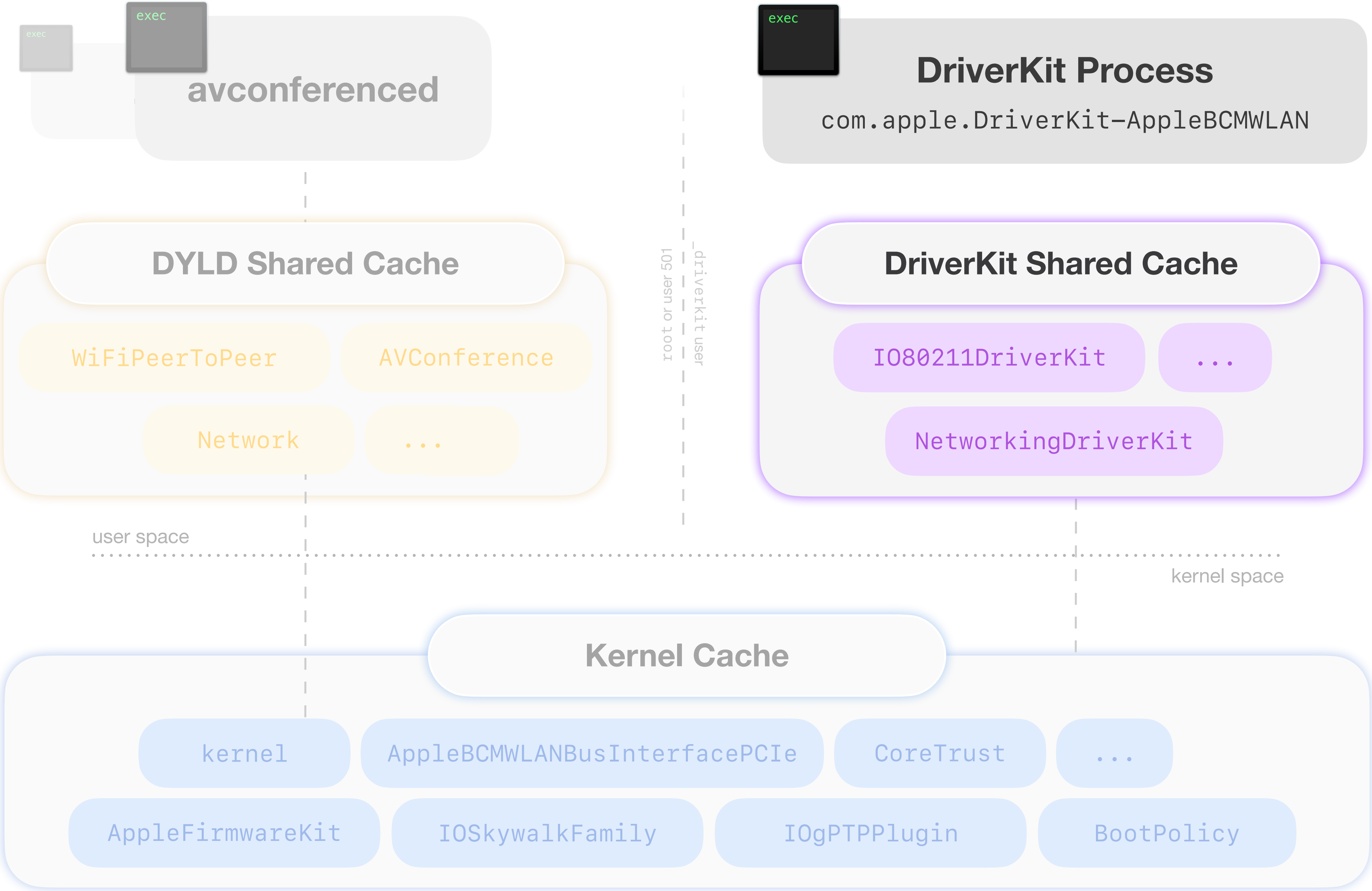
macOS

Firmware

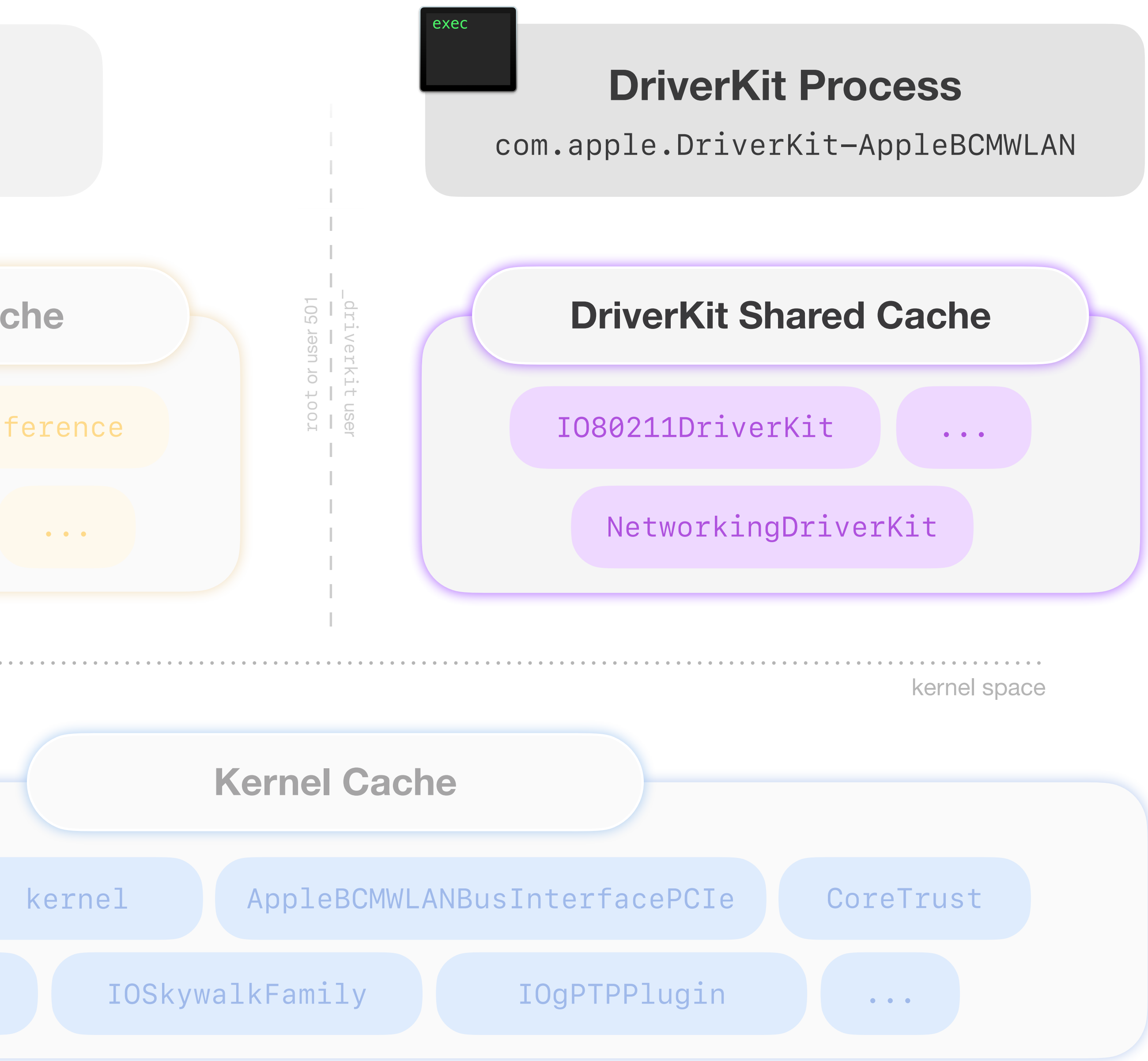


 **BROADCOM**
BCM84891LB01P
TN2224 P21
K522-01 B3 V

macOS



macOS



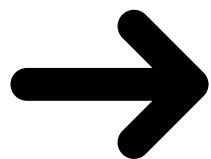
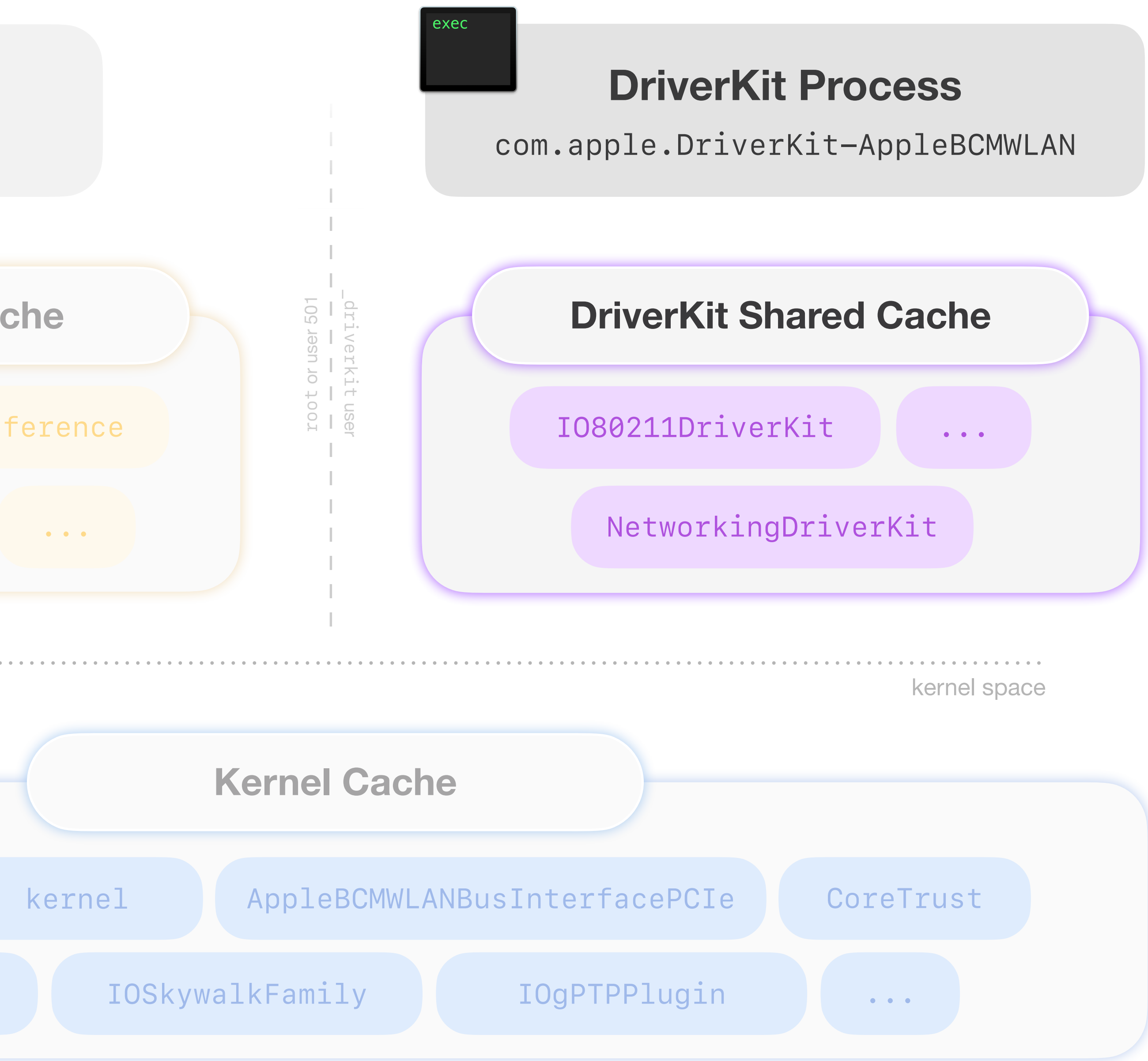
Networking-related tasks

Manages interfaces, queues

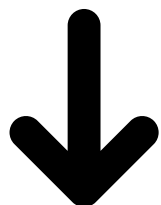
Handles IEEE 802.11 concepts

Configures wireless chips

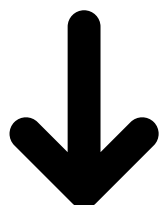
macOS



User-space process

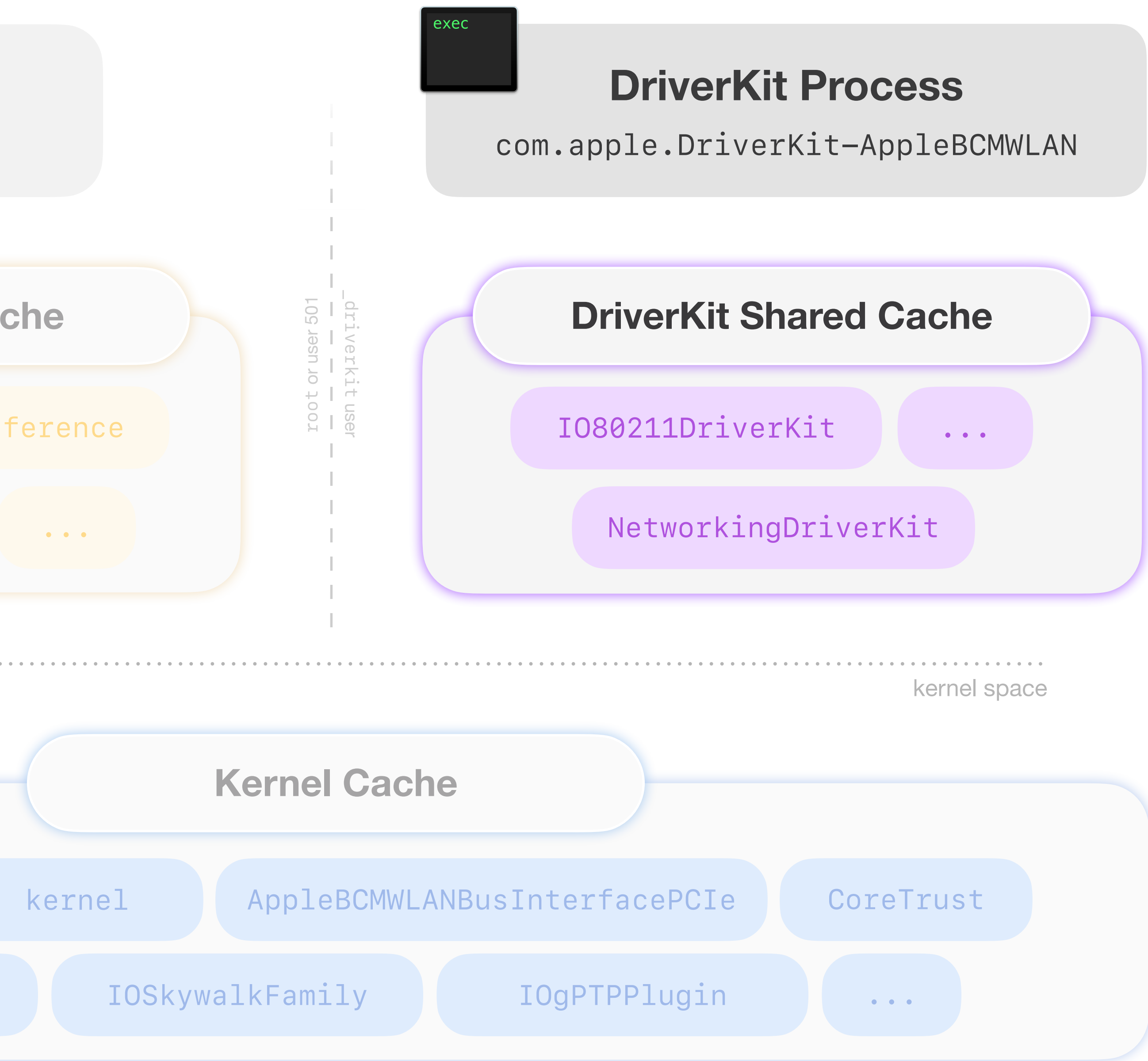


Great for LLDB debugging



Much more versatile than
kernel debugging

macOS



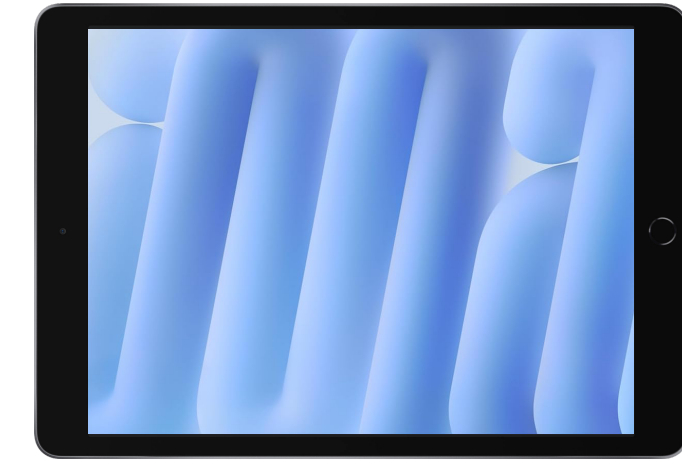
Interesting trace points: IOVARs

```
→ com.apple.Dr...MWLAN.arm64e × +
Symbols 🔍 IOVarGet × .* Aa
Name
AppleBCM WLANCommander::runIOVarGet(char const*, CommandTxPay.
AppleBCM WLANCommander::sendIOVarGet(char const*, CommandTxPa.
AppleBCM WLANCommander::runVirtualIOVarGet(uint8_t, char cons.
AppleBCM WLANCommander::sendVirtualIOVarGet(uint8_t, char con.
```

```
→ com.apple.Dr...MWLAN.arm64e × +
Symbols 🔍 image × .* Aa
Name
AppleBCM WLANCore::bootChipImage(AppleBCM WLANChipImage const*
AppleBCM WLANCore::verifyImages(I080211Buffer*, Ranges const&
AppleBCM WLANCore::logChipImage(AppleBCM WLANChipImage const*)
AppleBCM WLANCore::loadAndSetup(AppleBCM WLANChipImage const*)
AppleBCM WLANCore::setupFirmware(AppleBCM WLANChipImage const*
invocation function for block in AppleBCM WLANCore::setupFirm.
AppleBCM WLANBusInterfacePCie::allocChipImage(uint64_t, uint6.
non-virtual_thunk_to_AppleBCM WLANBusInterfacePCie::allocChip.
AppleBCM WLANBusInterfacePCie::generateChipImage(AppleBCM WLAN.
```



Sidecar Display



lldb



DriverKit Process

com.apple.DriverKit–AppleBCM WLAN

DriverKit Shared Cache

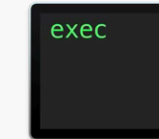
I080211DriverKit

...

NetworkingDriverKit



lldb



DriverKit Process

com.apple.DriverKit–AppleBCM WLAN

DriverKit Shared Cache

I080211DriverKit

...

NetworkingDriverKit

Tracing wireless chip configuration

macOS

Firmware

Kit Process

verKit-AppleBCM WLAN

AppleBCM WLAN Proximity Inter
face::createChipInterface

Shared Cache

verKit

...

ingDriverKit

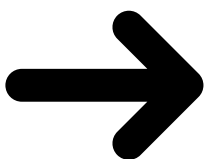
kernel space

CoreTrust

...

"interface_create"

Payload

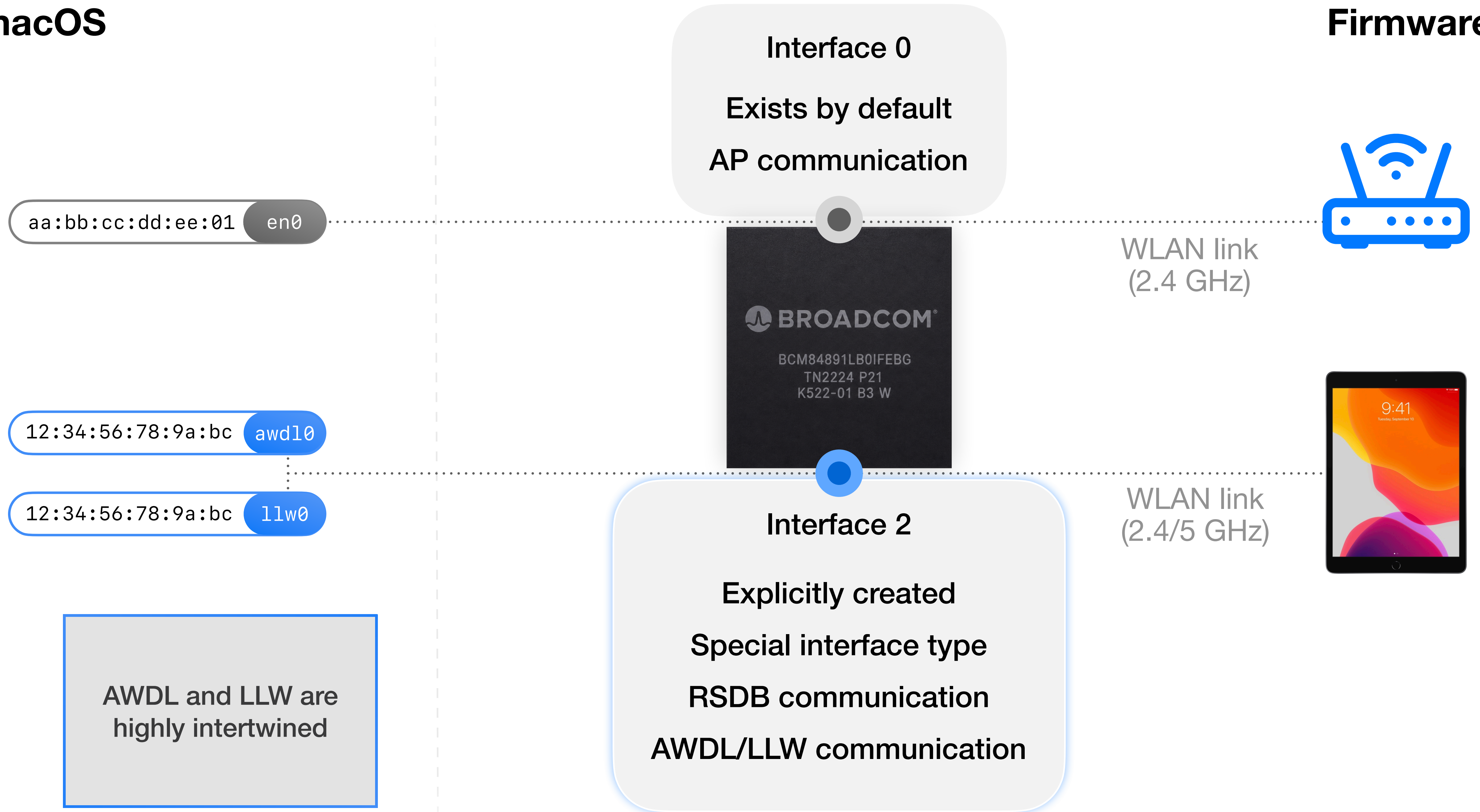


BROADCOM

BCM84891LB01P
TN2224 P21
K522-01 B3 V

macOS

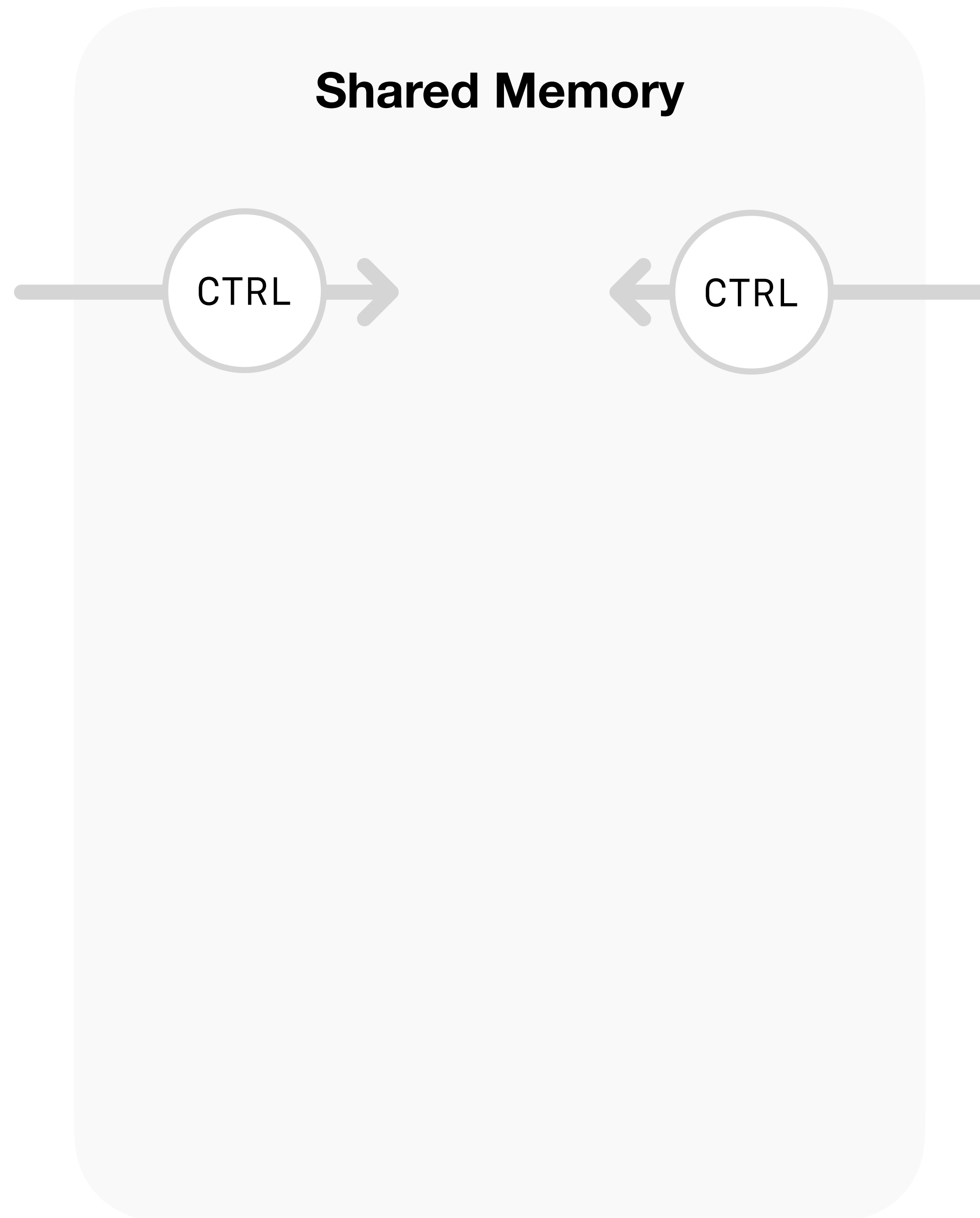
Firmware



macOS

Firmware

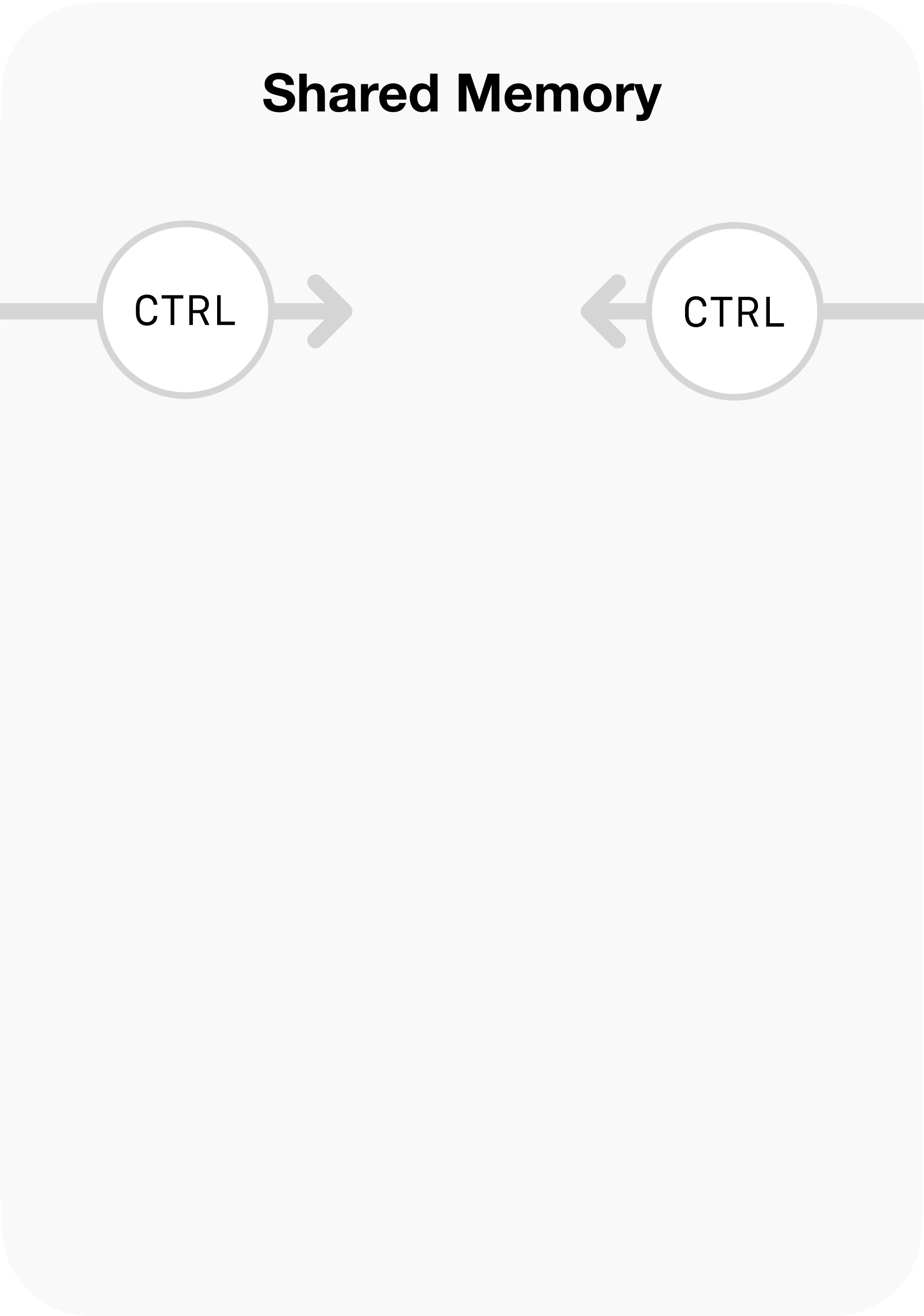

msgbuf messages



→ Submission Ring (H2D)
← Completion Ring (D2H)

macOS

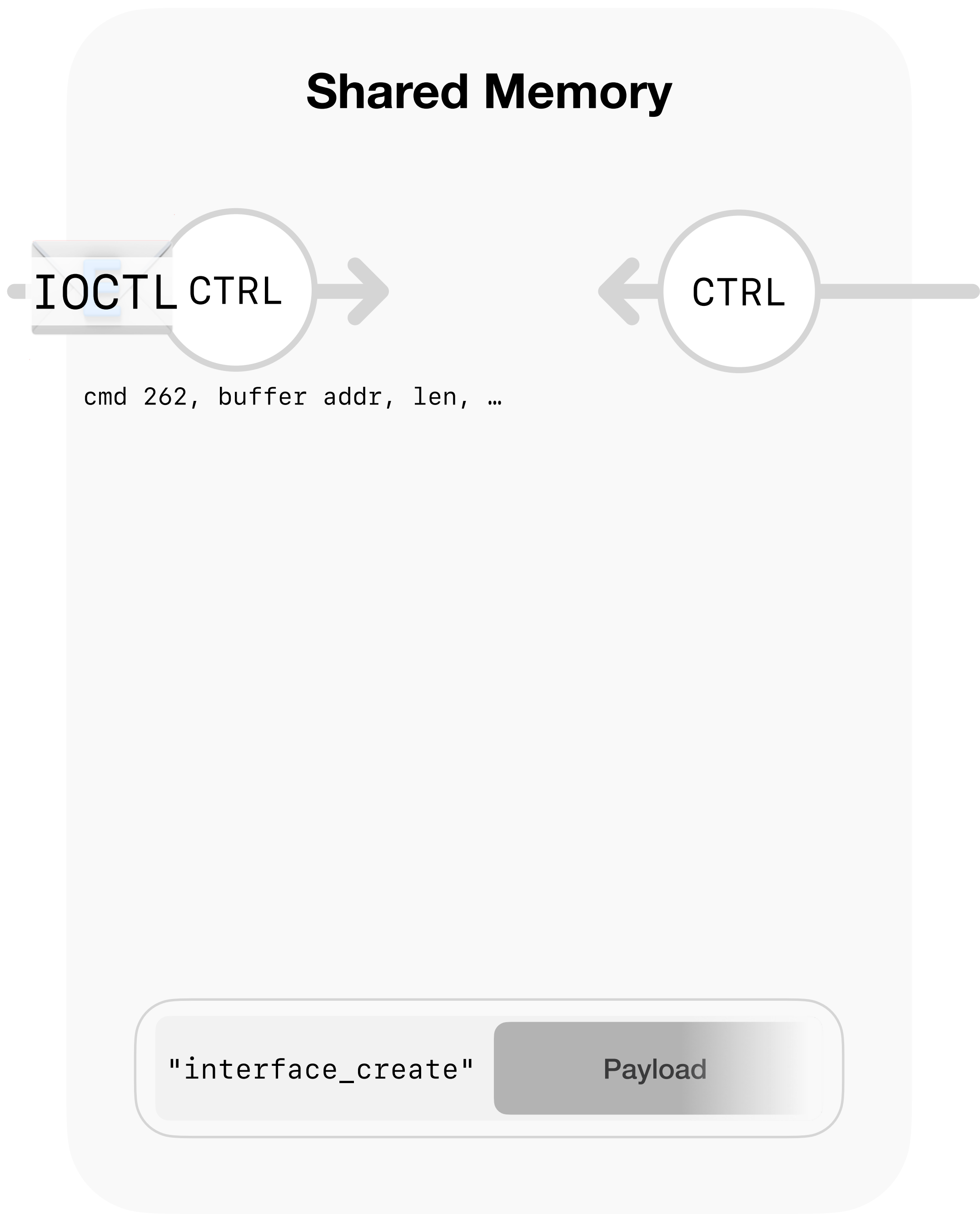
Firmware



"interface_create"

Payload

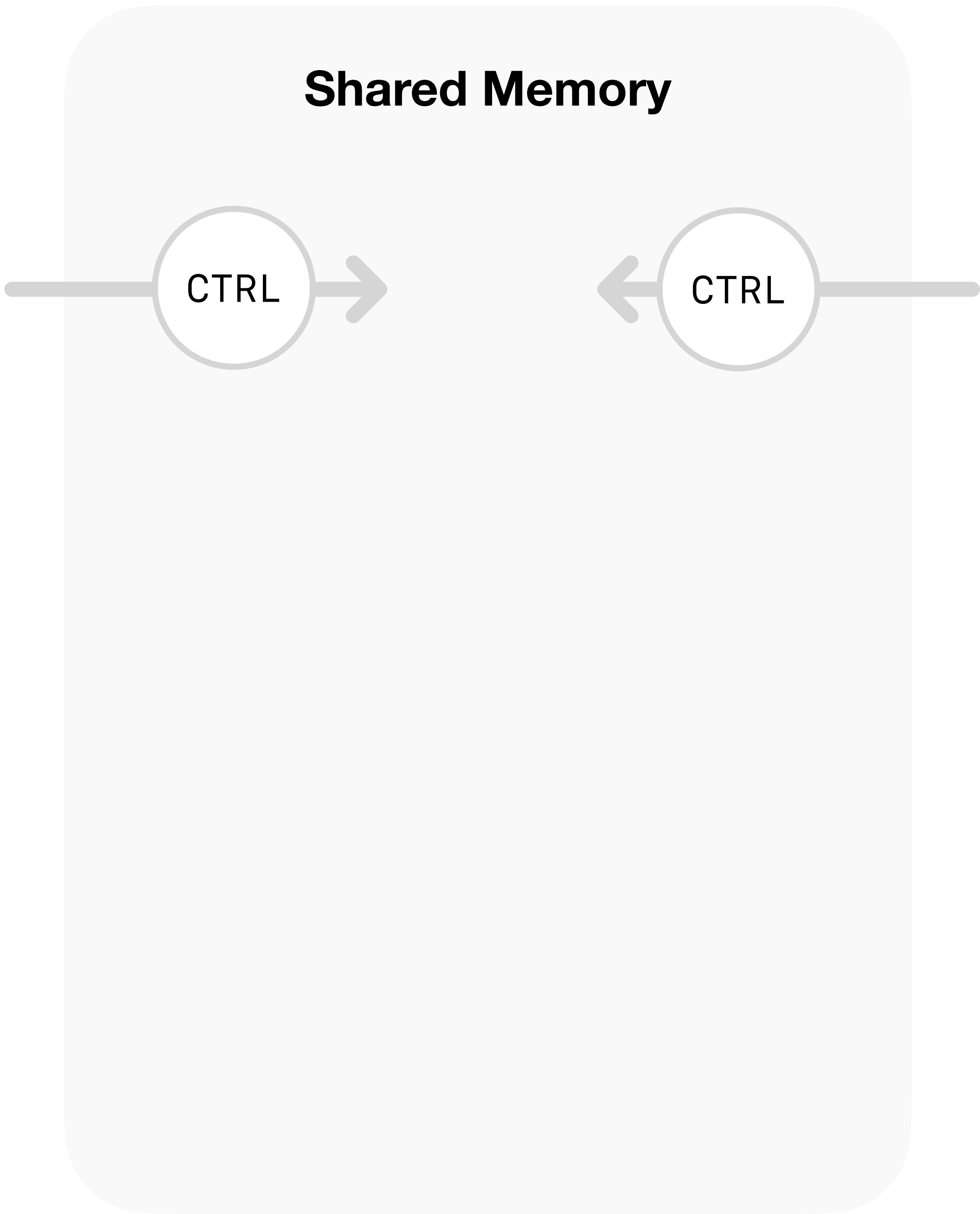
- Submission Ring (H2D)
- ← Completion Ring (D2H)



→ Submission Ring (H2D)
← Completion Ring (D2H)

macOS

Firmware

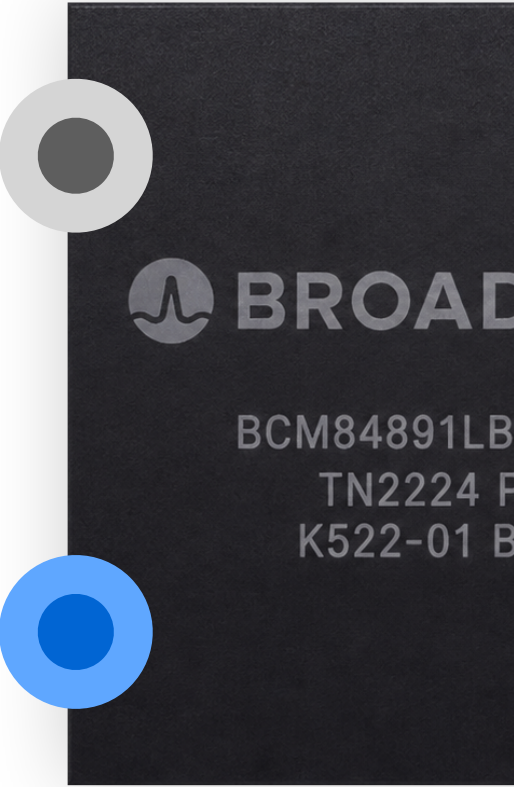
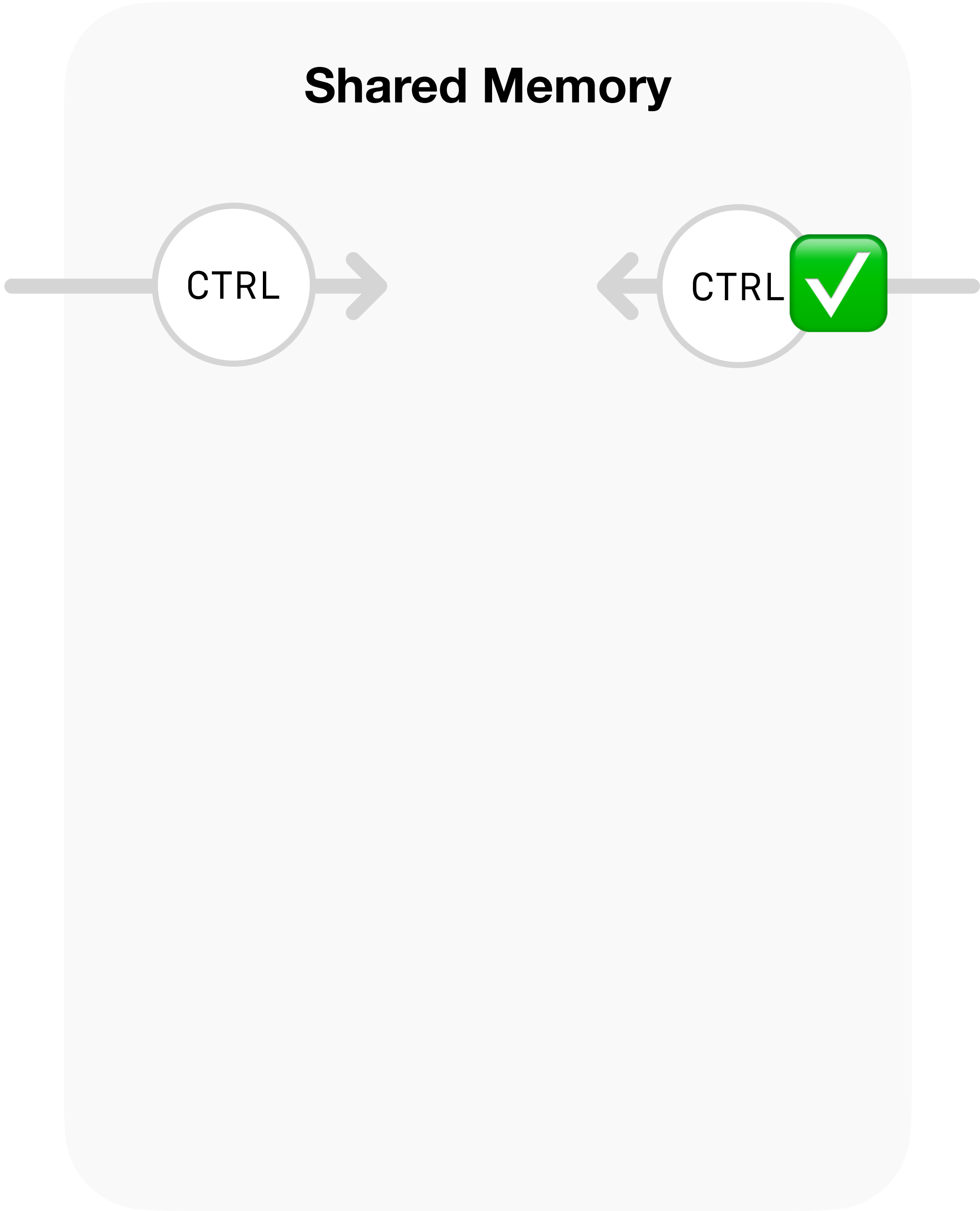


"interface_create"

- Submission Ring (H2D)
- ← Completion Ring (D2H)

macOS

Firmware

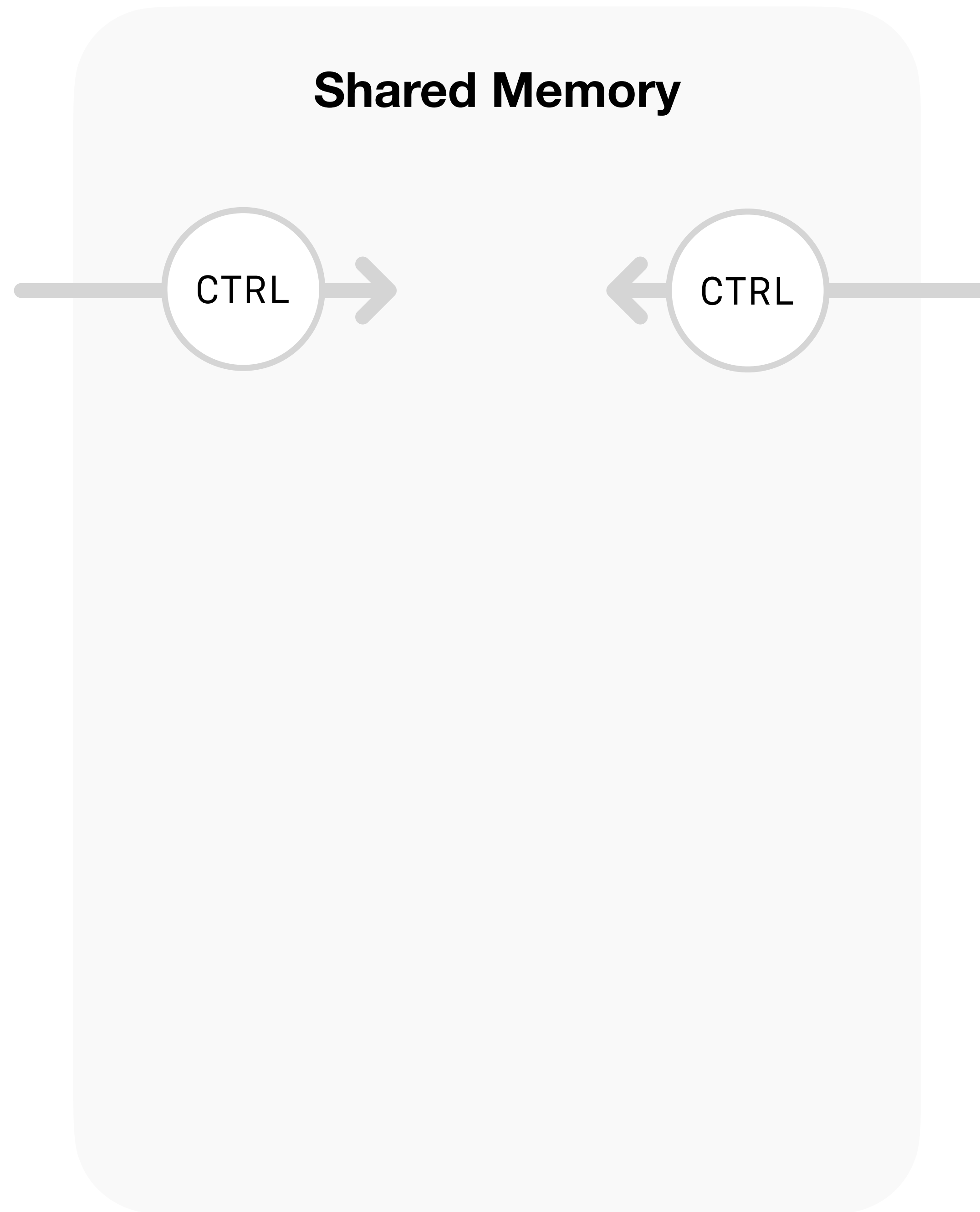


→ Submission Ring (H2D)
← Completion Ring (D2H)

macOS

Firmware

Configuration
IOCTLs and more



→ Submission Ring (H2D)
← Completion Ring (D2H)

DriverKit Process

DriverKit-AppleBCM WLAN

AppleBCM WLAN Proximity Interface::createChipInterface

DriverKit Shared Cache

DriverKit

...

WorkingDriverKit

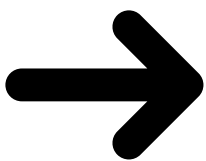
kernel space

CoreTrust

...

"interface_create"

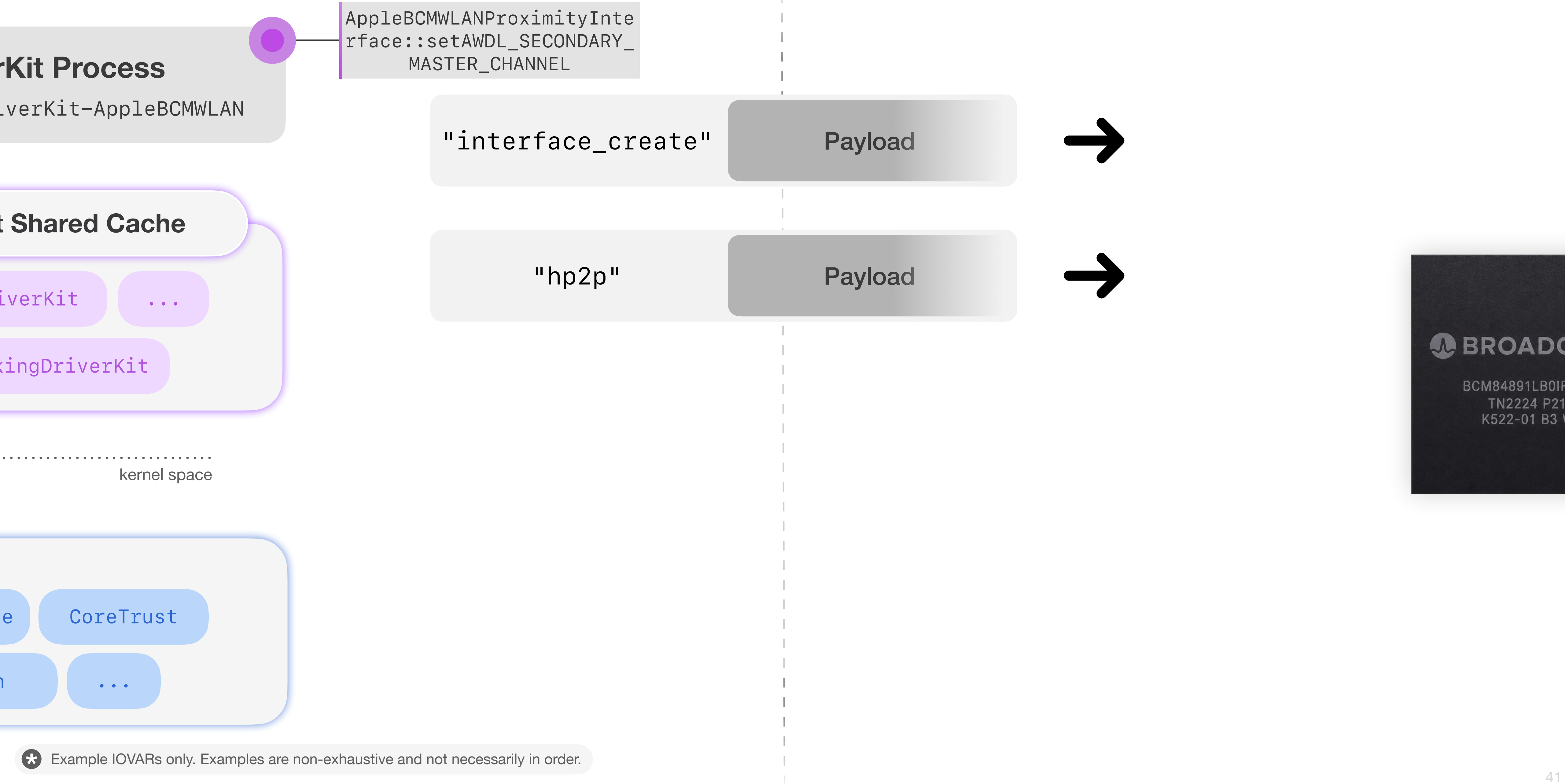
Payload

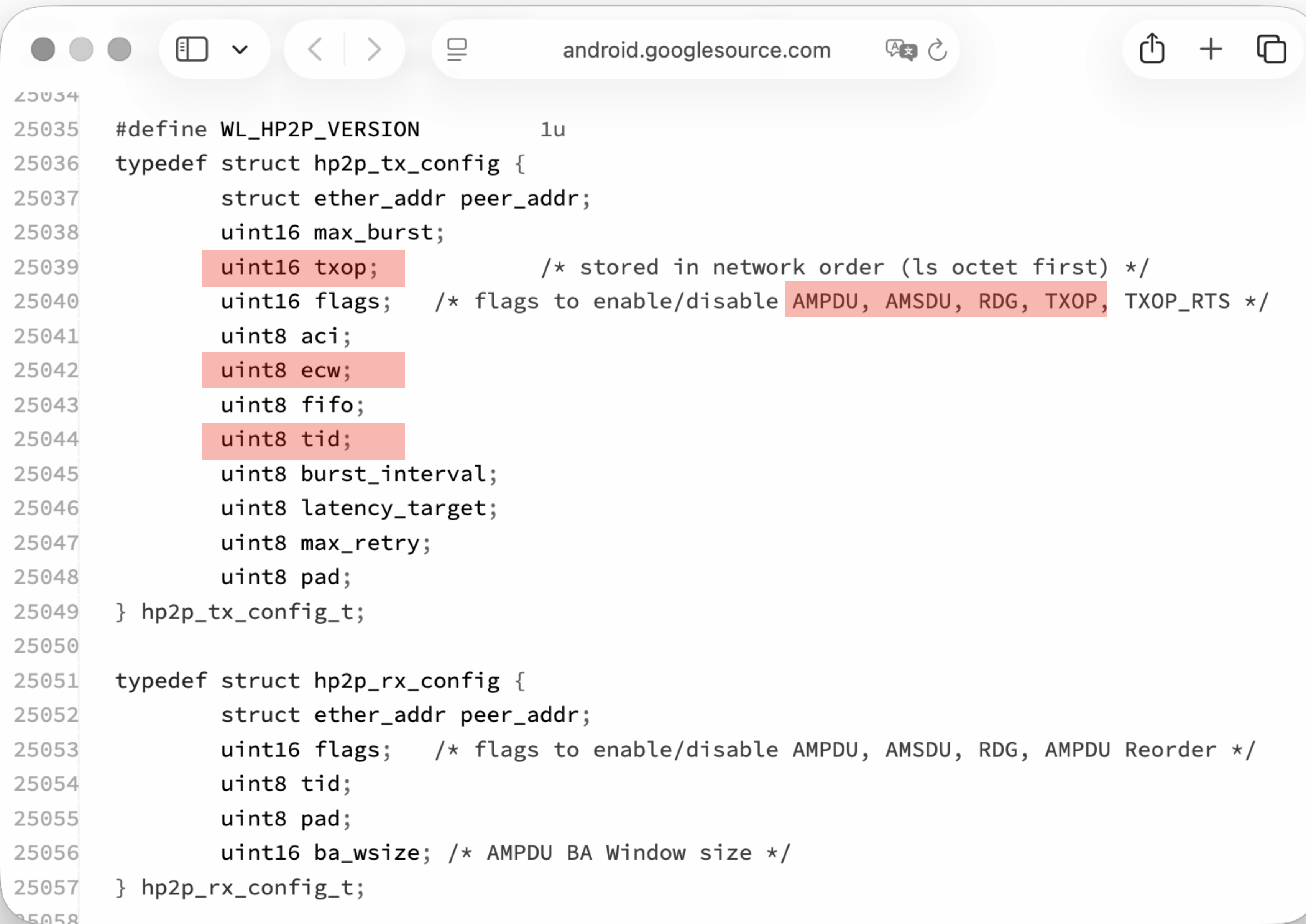


* Example IOVARs only. Examples are non-exhaustive and not necessarily in order.

macOS

Firmware





```
25034
25035 #define WL_HP2P_VERSION          1u
25036 typedef struct hp2p_tx_config {
25037     struct ether_addr peer_addr;
25038     uint16 max_burst;
25039     uint16 txop;                /* stored in network order (ls octet first) */
25040     uint16 flags; /* flags to enable/disable AMPDU, AMSDU, RDG, TXOP, TXOP_RTS */
25041     uint8 aci;
25042     uint8 ecw;
25043     uint8 fifo;
25044     uint8 tid;
25045     uint8 burst_interval;
25046     uint8 latency_target;
25047     uint8 max_retry;
25048     uint8 pad;
25049 } hp2p_tx_config_t;
25050
25051 typedef struct hp2p_rx_config {
25052     struct ether_addr peer_addr;
25053     uint16 flags; /* flags to enable/disable AMPDU, AMSDU, RDG, AMPDU Reorder */
25054     uint8 tid;
25055     uint8 pad;
25056     uint16 ba_wsize; /* AMPDU BA Window size */
25057 } hp2p_rx_config_t;
25058
```

DriverKit Process

DriverKit-AppleBCM WLAN

Shared Cache

DriverKit

...

WorkingDriverKit

kernel space

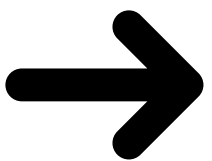
CoreTrust

...

AppleBCM WLAN Proximity Interface::setAWDL_SYNC_STATE

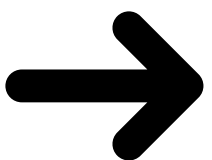
"interface_create"

Payload



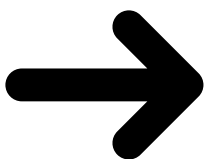
"hp2p"

Payload



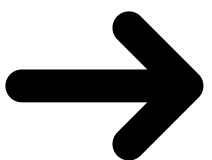
"slot_bss"

Payload



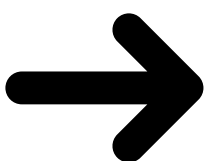
"awdl_sync_params"

Payload



"awdl_opmode"

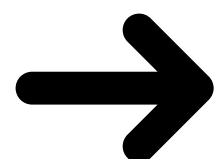
Payload



* Example IOVARs only. Examples are non-exhaustive and not necessarily in order.

Bringing Low-Latency WiFi to Linux

macOS



Linux

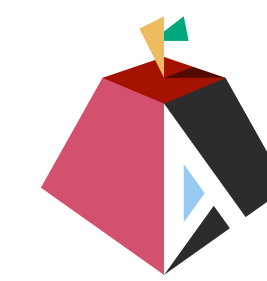
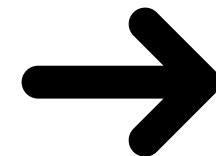
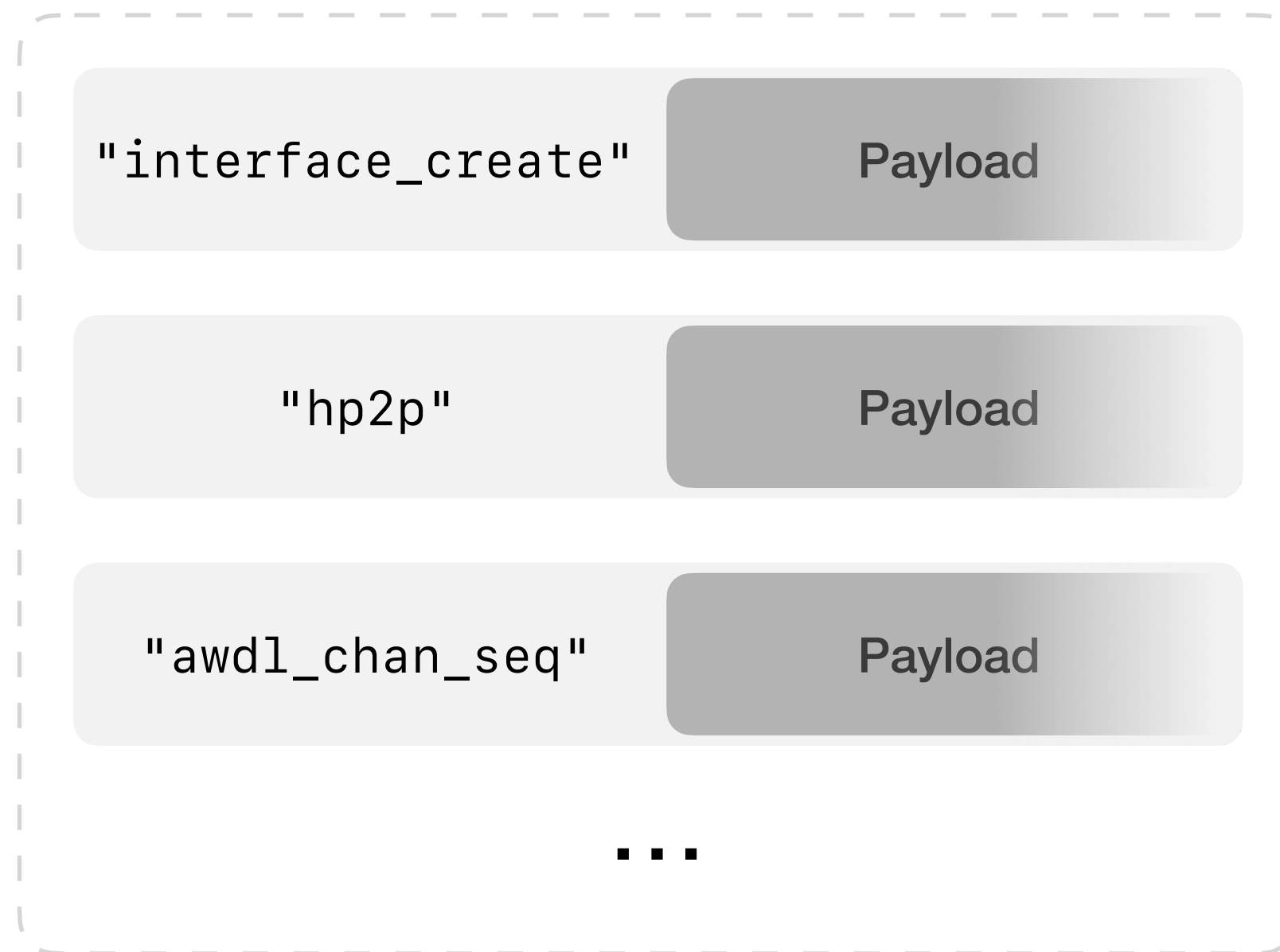


Different Broadcom chips

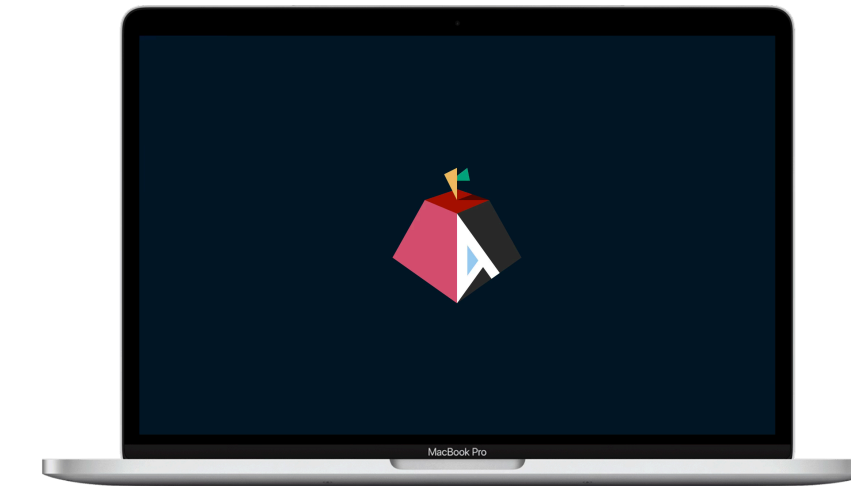
Different Firmware

No support for proprietary IOVARs

macOS



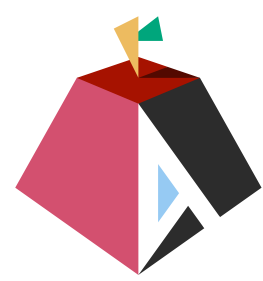
Linux



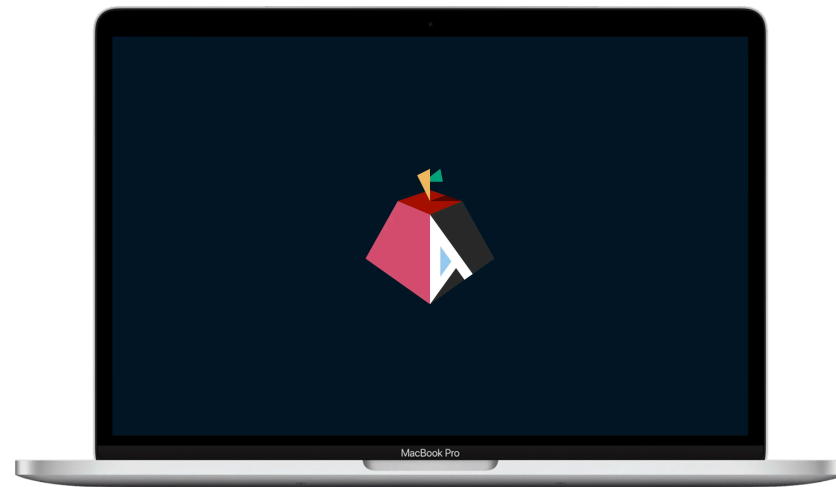
Runs on Apple hardware

Same hardware for tracing and testing

Uses macOS' firmwares



Linux



cfg80211

nl80211

core

chan

util

brcmfmac

core

interface_create

flowring

pcie

awdl

awdl_iovars

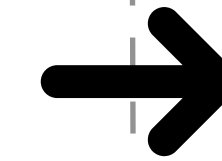
cfg80211

commonring

msgbuf

bus

llw



Firmware



"interface_create"

Payload

"hp2p"

Payload

"awdl_chan_seq"

Payload

...

BROADCOM
BCM84891LB01H
TN2224 P21
K522-01 B3

Extending the Broadcom **driver**

Configuration

IOCTLs, flowring creation, and more

AP communication

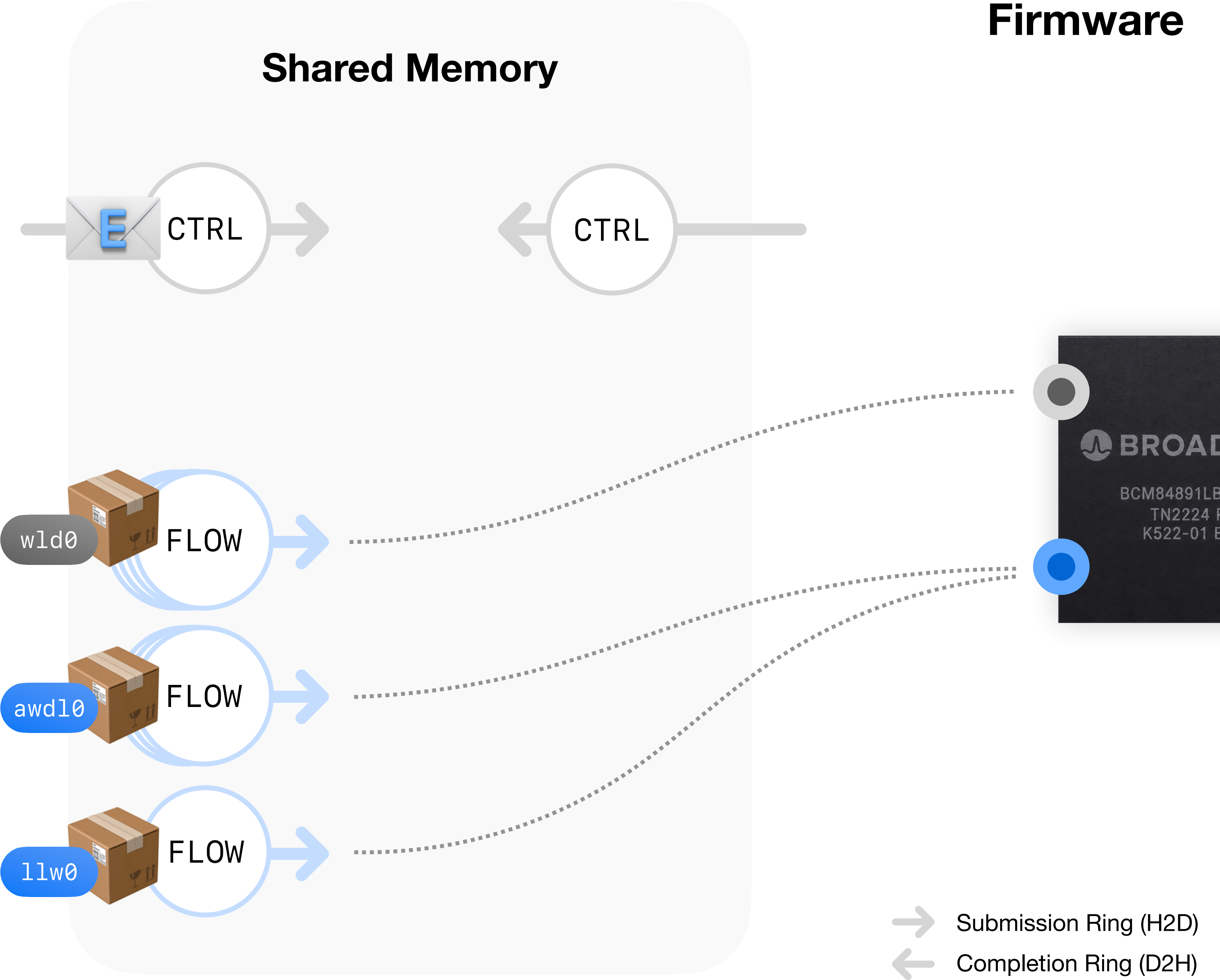
Background, Best Effort, Voice, Video

AWDL traffic

Background, Best Effort, Voice (TID 6)

LLW traffic

Voice (TID 7)



	Access Category	Traffic Identifier	Protocol
Priority (channel access) ↓	Background	1	AWDL
	Background	2	
	Best Effort	0	
	Best Effort	3	
	Video	4	
	Video	5	
	Voice	6	LLW
	Voice	7	

- Configuration

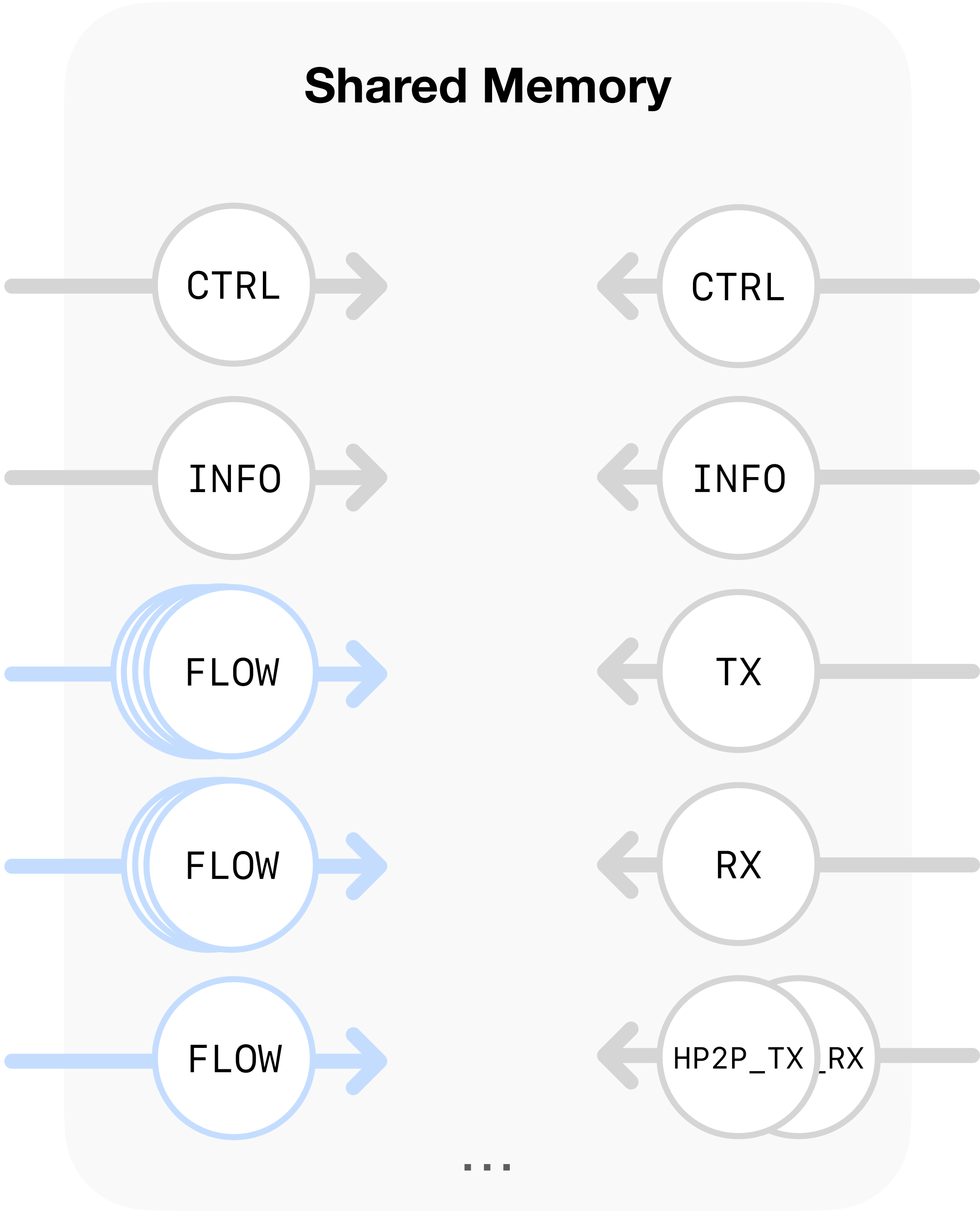
IOCTLs, flowring creation, and more
- Debug information

(assumably)
- AP communication

Background, Best Effort, Voice, Video
- AWDL traffic

Background, Best Effort, Voice (TID 6)
- LLW traffic

Voice (TID 7)



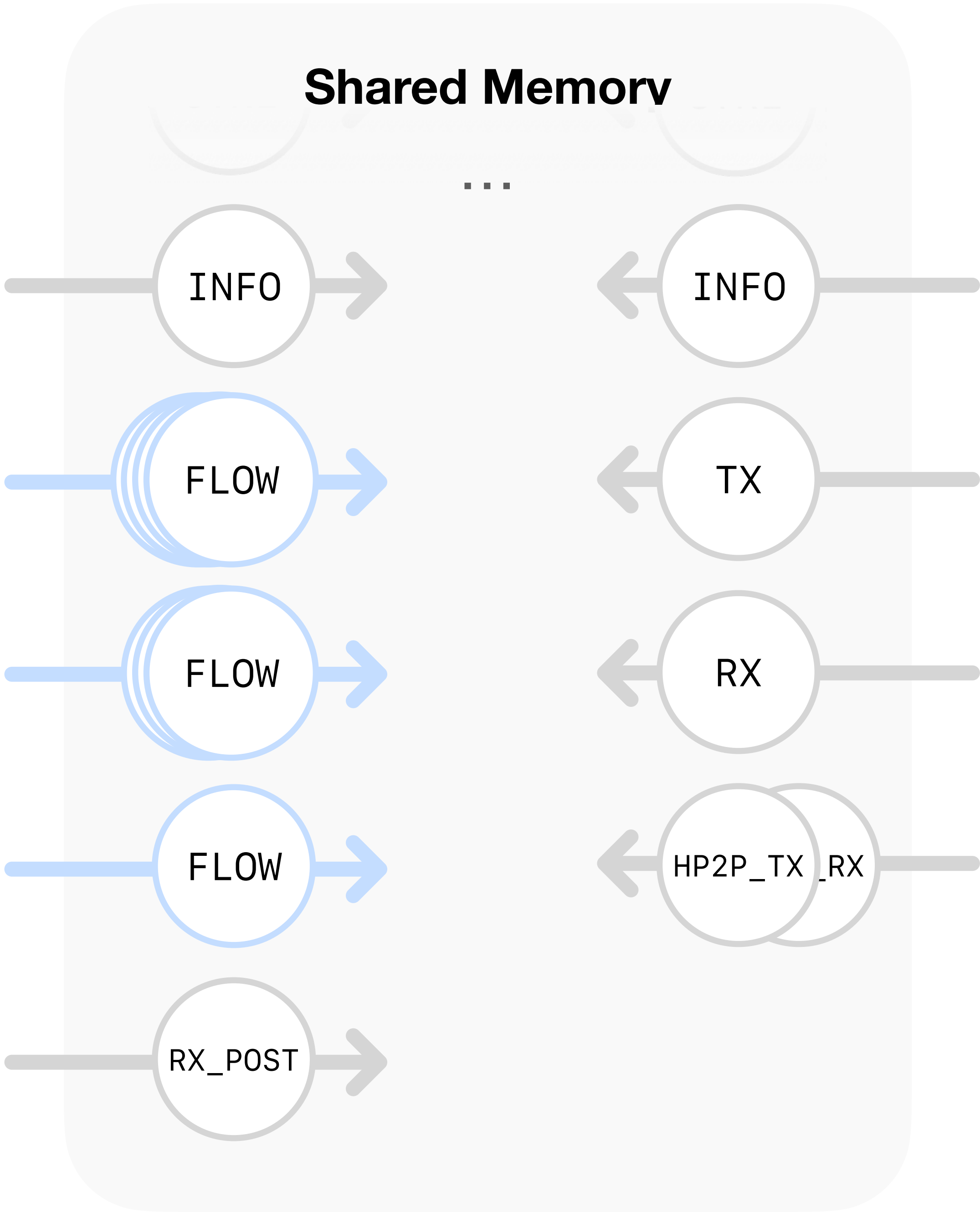
Debug information
(assumably)

AP communication
Background, Best Effort, Voice, Video

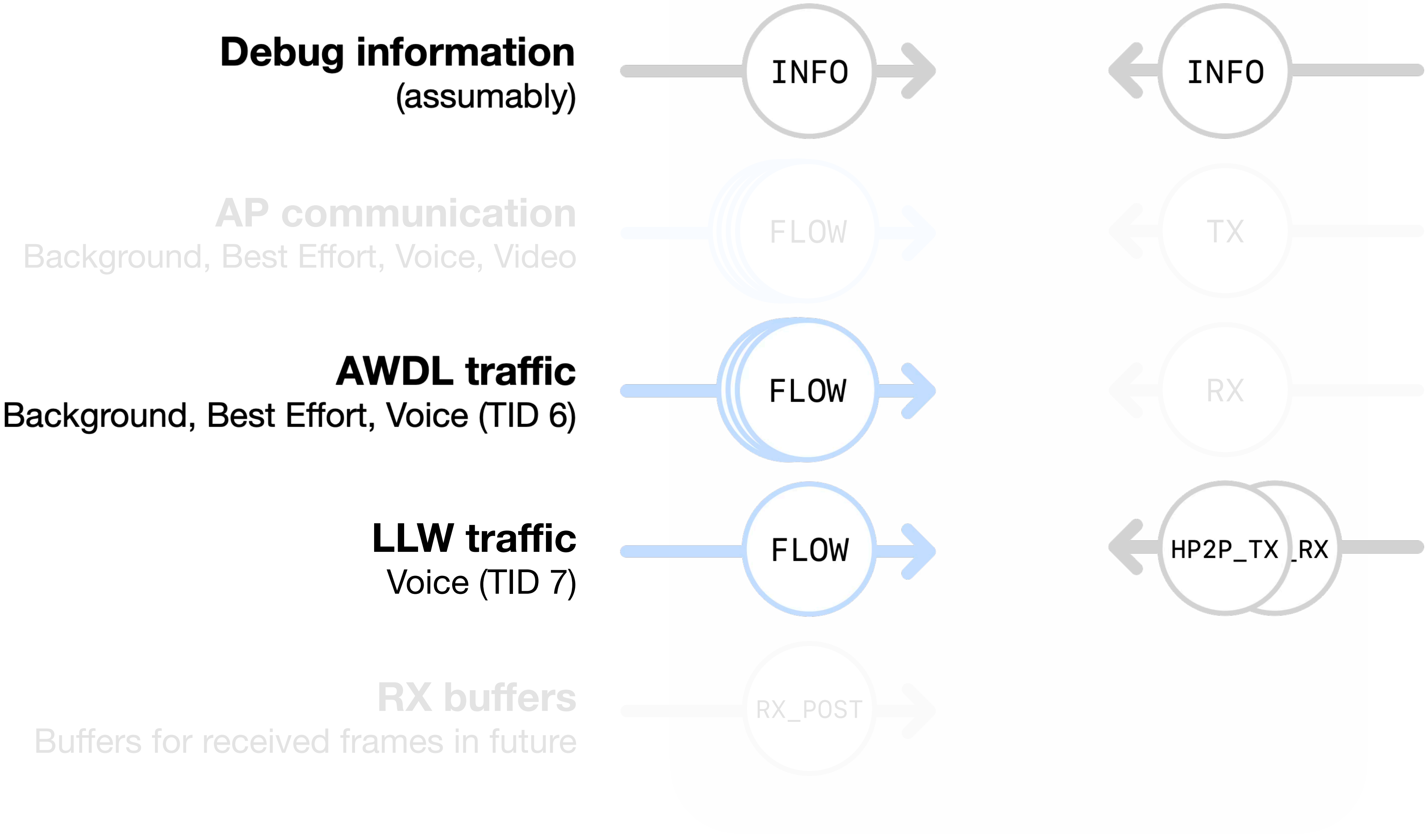
AWDL traffic
Background, Best Effort, Voice (TID 6)

LLW traffic
Voice (TID 7)

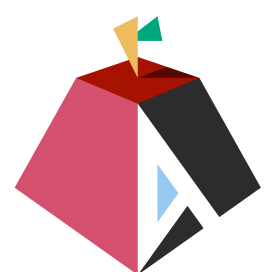
RX buffers
Buffers for received frames in future



→ Submission Ring (H2D)
← Completion Ring (D2H)



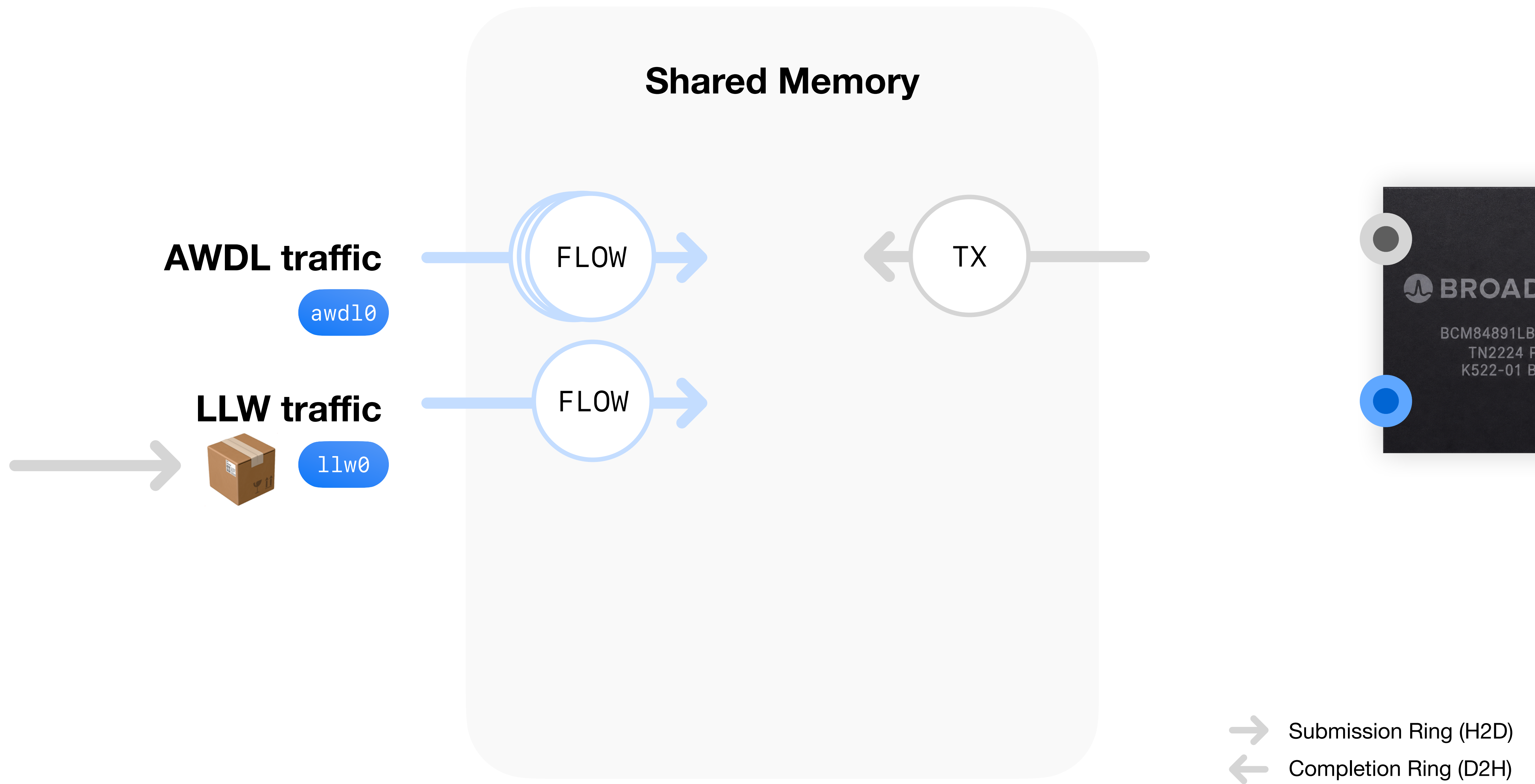
Sending and receiving traffic

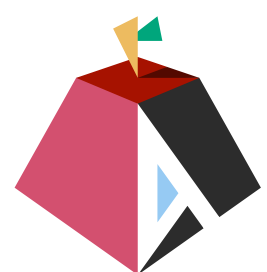


Linux

Sending Traffic via 11w0

Firmware

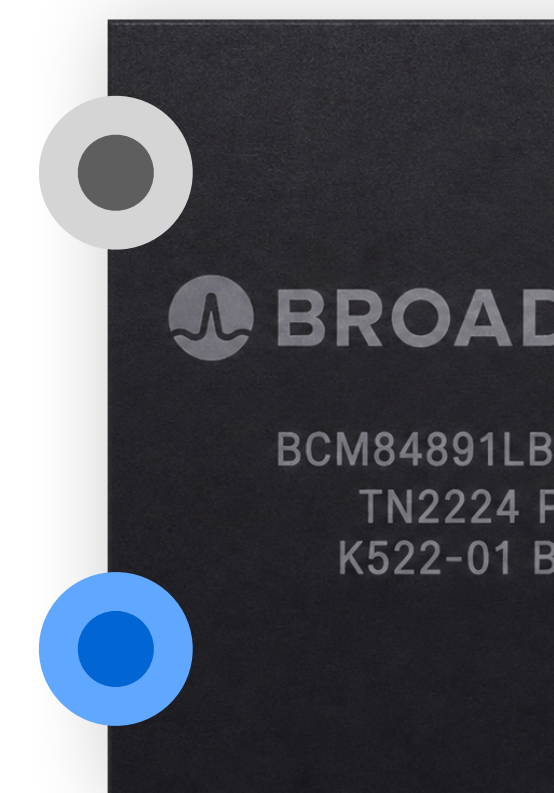
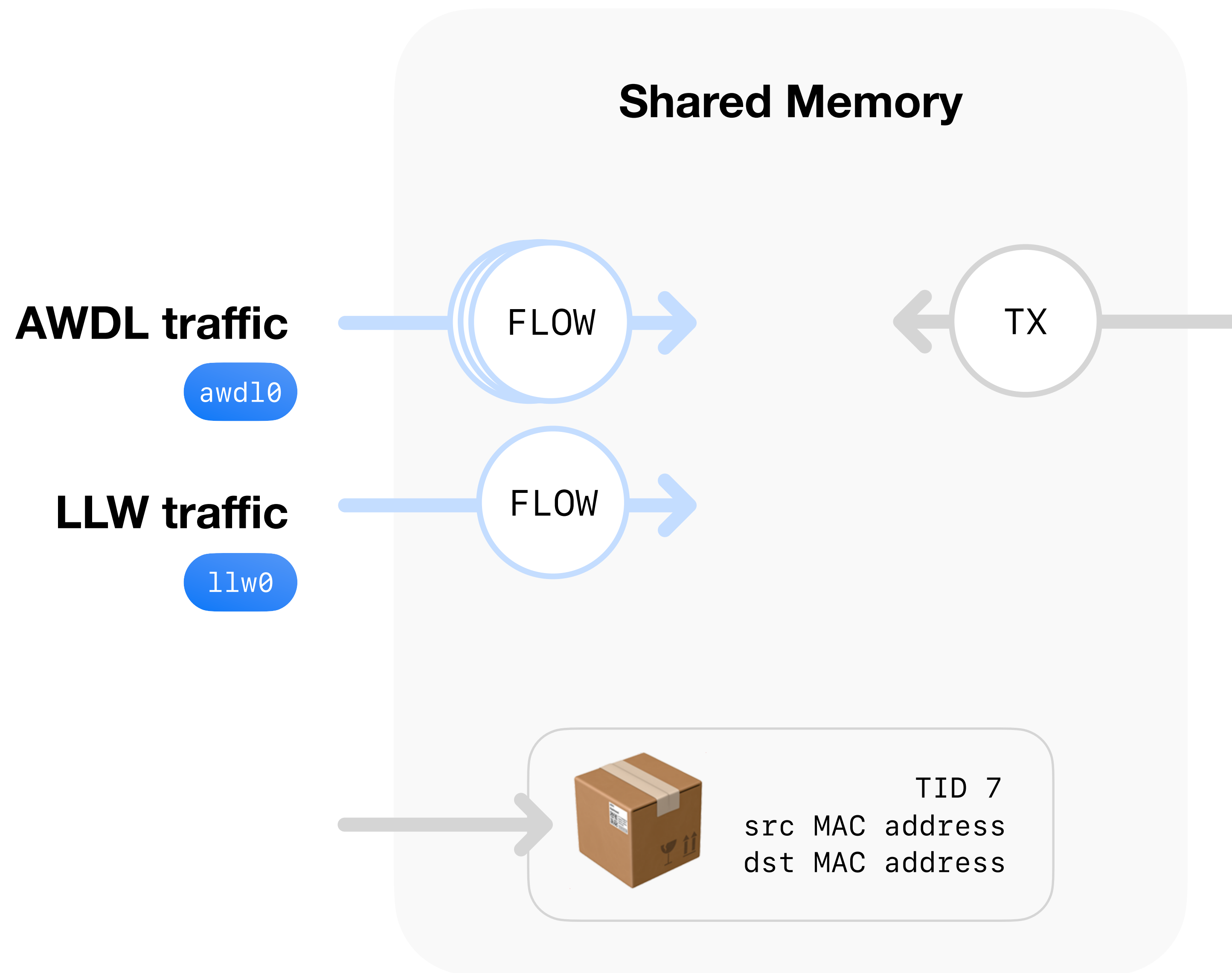




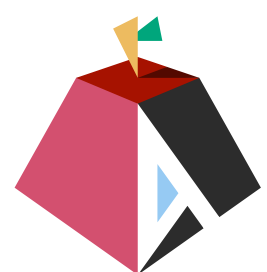
Linux

Sending Traffic via 11w0

Firmware



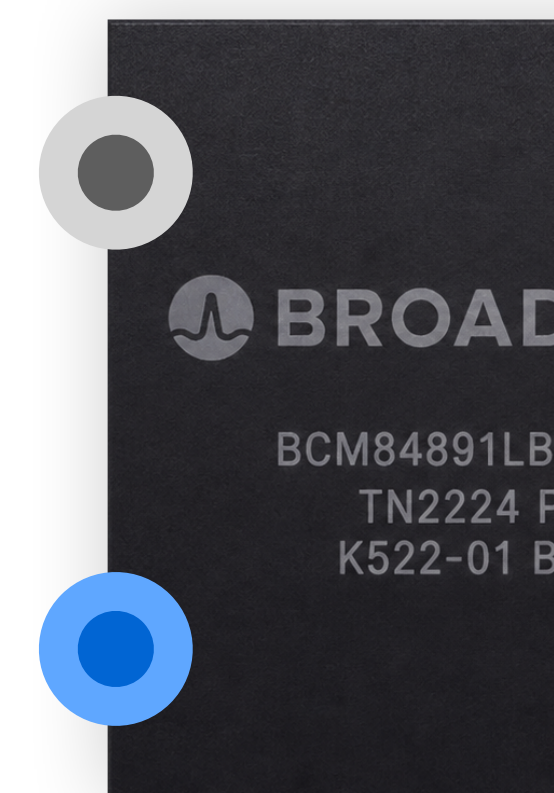
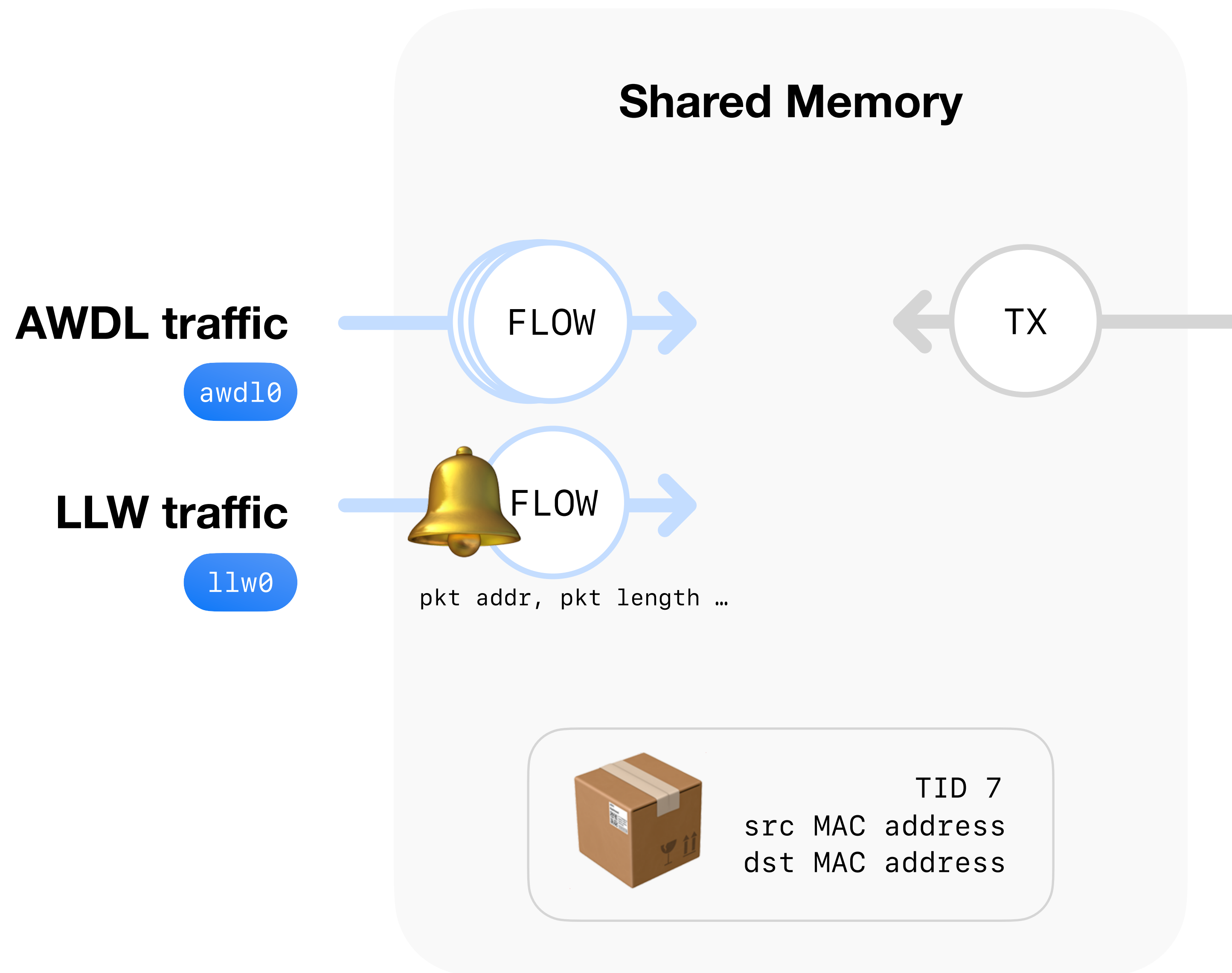
→ Submission Ring (H2D)
← Completion Ring (D2H)



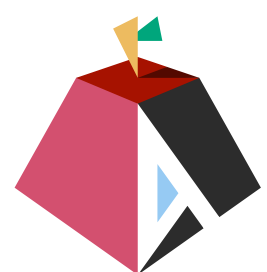
Linux

Sending Traffic via 11w0

Firmware



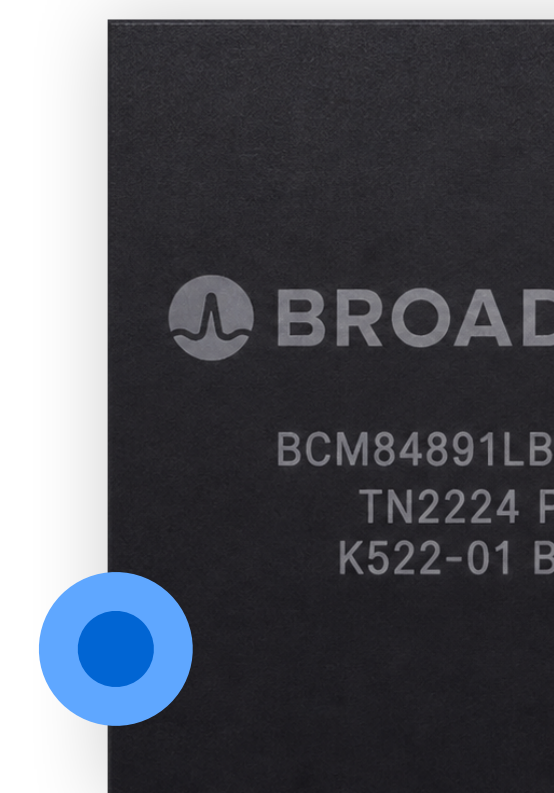
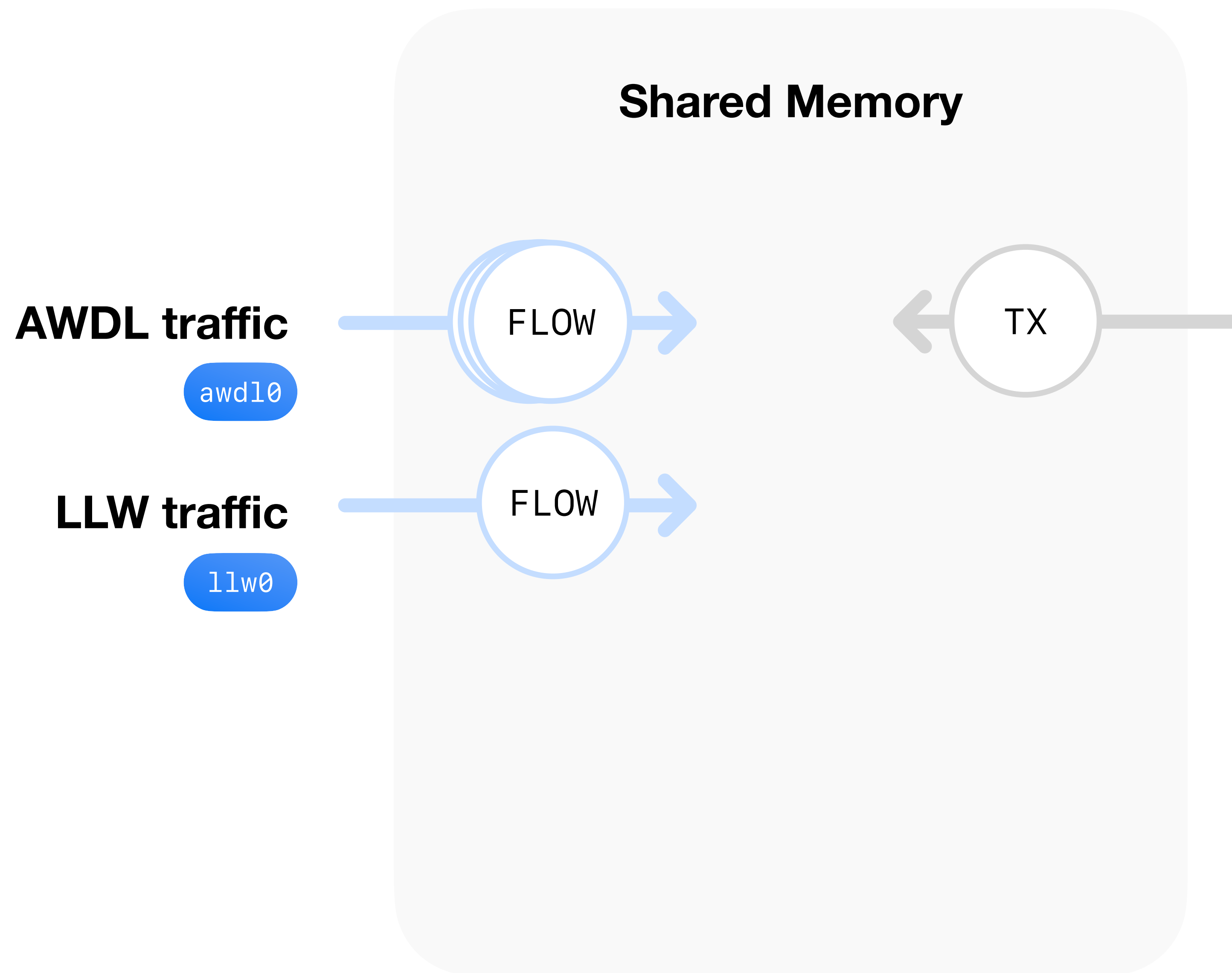
→ Submission Ring (H2D)
← Completion Ring (D2H)



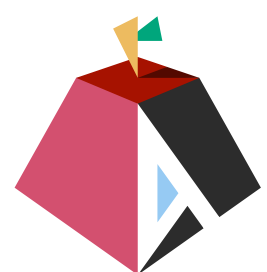
Linux

Sending Traffic via 11w0

Firmware



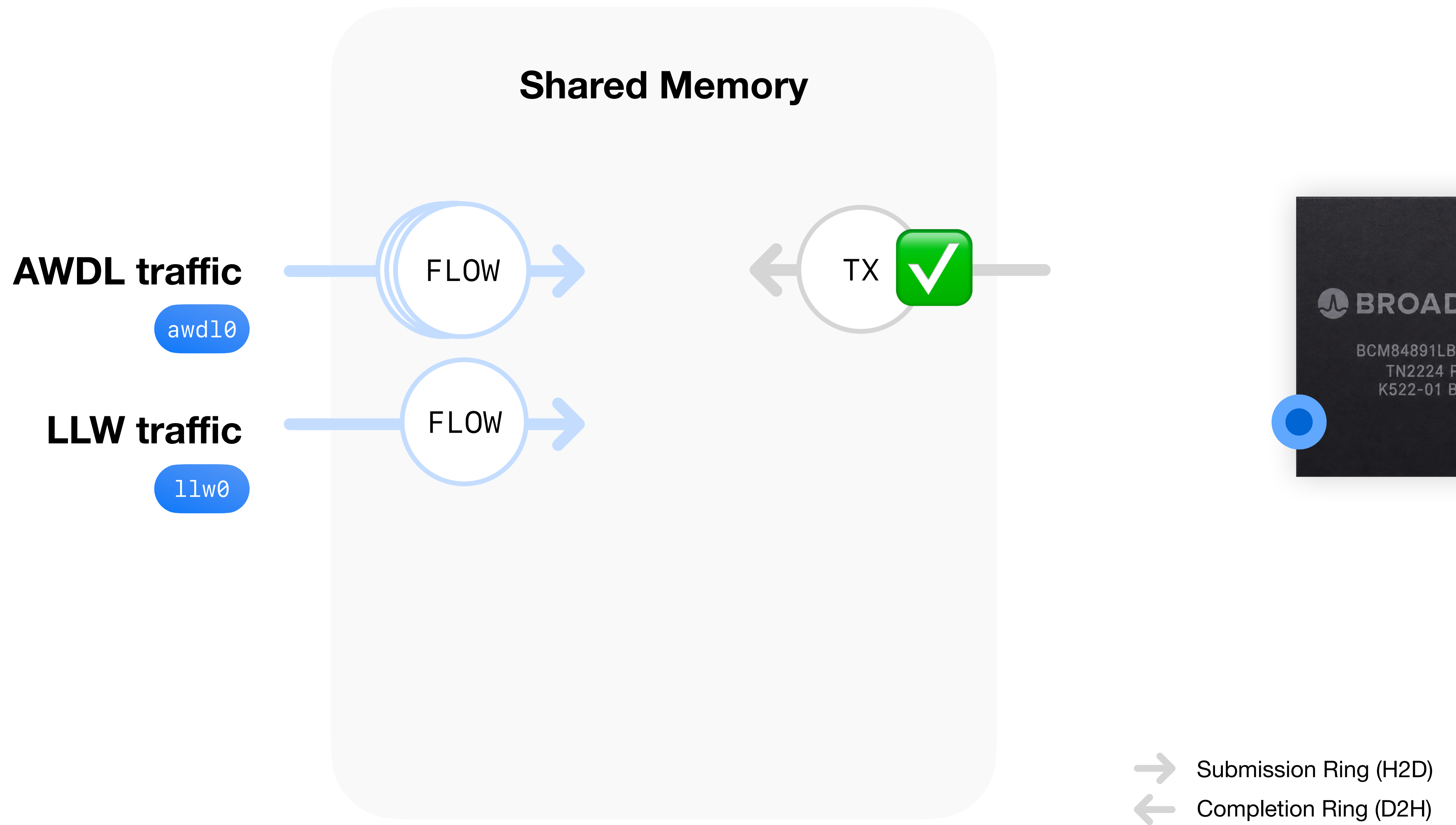
→ Submission Ring (H2D)
← Completion Ring (D2H)

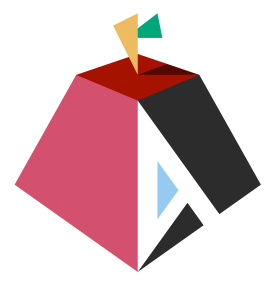


Linux

Sending Traffic via 11w0

Firmware





Linux

Receiving Traffic via awd10/11w0

Firmware

Shared Memory

AP communication

aa:bb:cc:dd:ee:01 wld0

AWDL traffic

12:34:56:78:9a:bc awd10

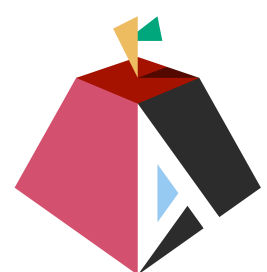
LLW traffic

12:34:56:78:9a:bc llw0

BROAD

BCM84891LB
TN2224 F
K522-01 B

→ Submission Ring (H2D)
← Completion Ring (D2H)



Linux

Receiving Traffic via awd10/11w0

Firmware

Shared Memory

AP communication

aa:bb:cc:dd:ee:01 wld0

AWDL traffic

12:34:56:78:9a:bc awd10

LLW traffic

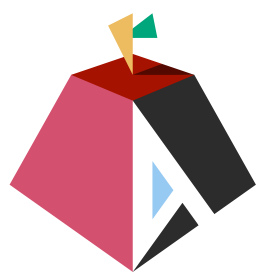
12:34:56:78:9a:bc llw0

BROAD

BCM84891LB
TN2224 F
K522-01 B



→ Submission Ring (H2D)
← Completion Ring (D2H)



Linux

Receiving Traffic via awd10/11w0

Firmware

AP communication

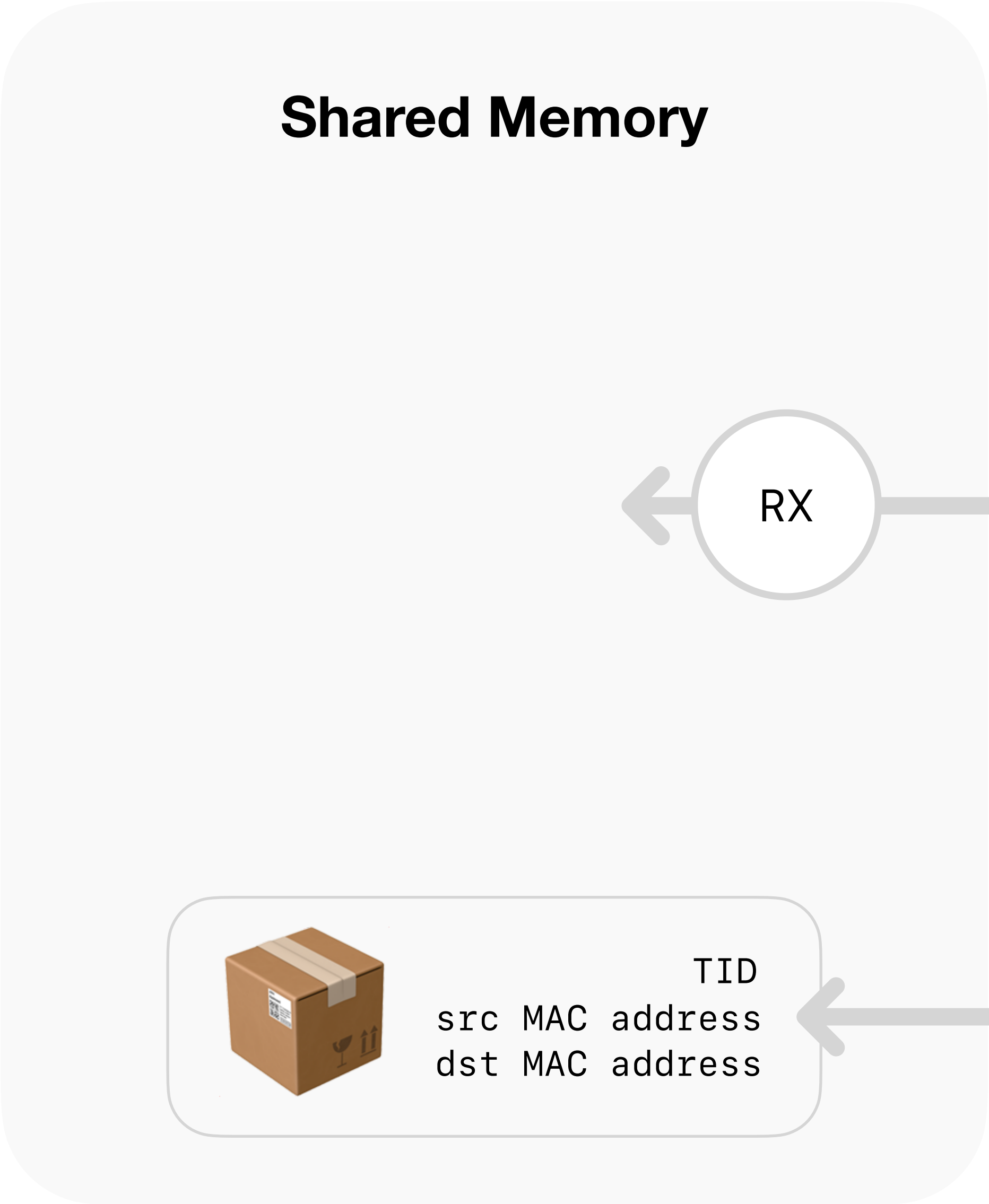
aa:bb:cc:dd:ee:01 wld0

AWDL traffic

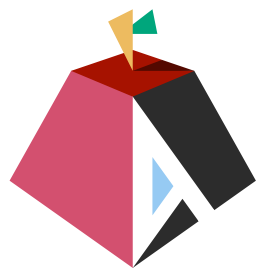
12:34:56:78:9a:bc awd10

LLW traffic

12:34:56:78:9a:bc llw0



→ Submission Ring (H2D)
← Completion Ring (D2H)



Linux

Receiving Traffic via awd10/11w0

Firmware

AP communication

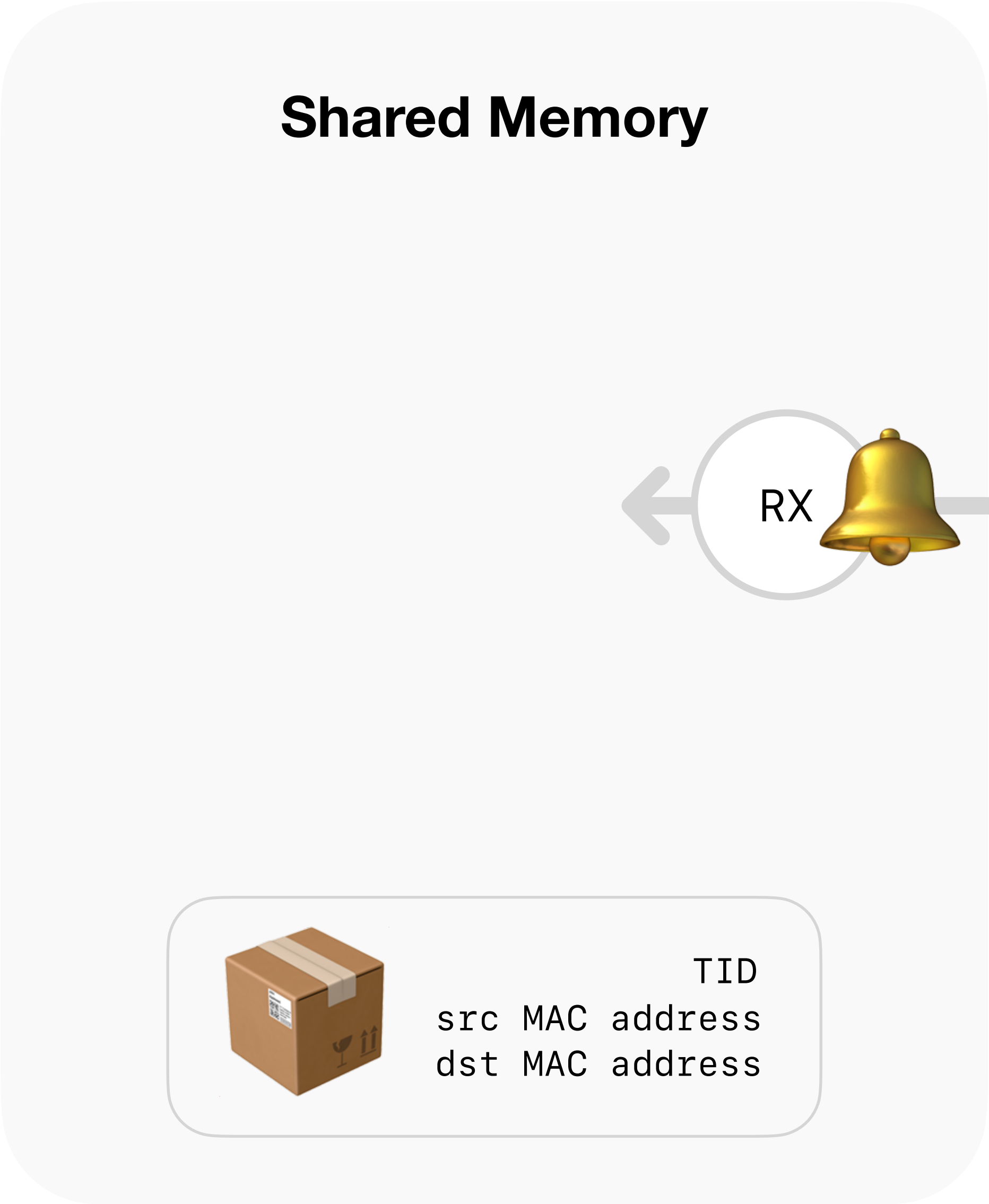
aa:bb:cc:dd:ee:01 wld0

AWDL traffic

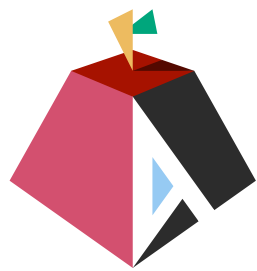
12:34:56:78:9a:bc awd10

LLW traffic

12:34:56:78:9a:bc llw0



→ Submission Ring (H2D)
← Completion Ring (D2H)



Linux

Receiving Traffic via awd10/11w0

Firmware

AP communication

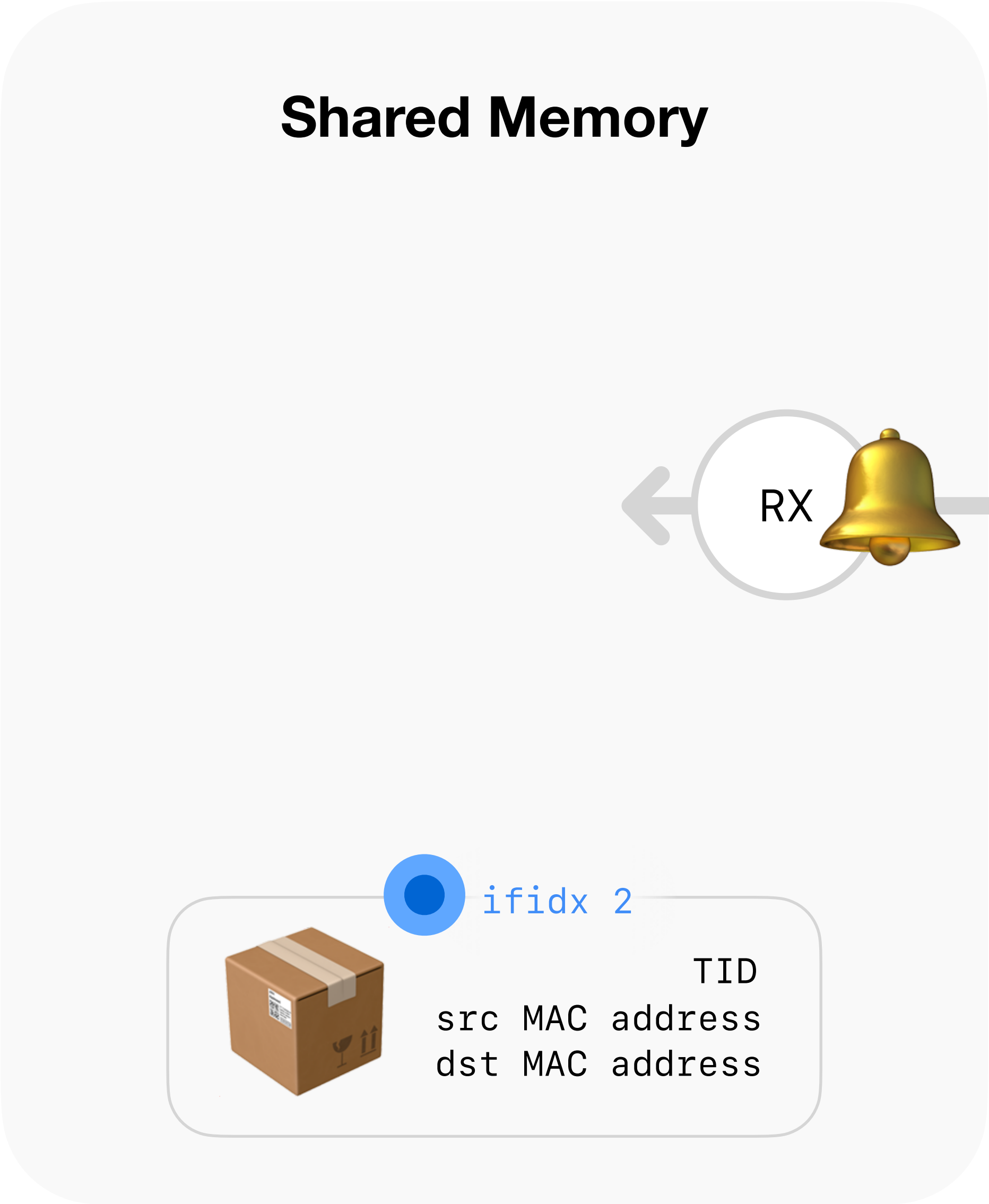
aa:bb:cc:dd:ee:01 wld0

AWDL traffic

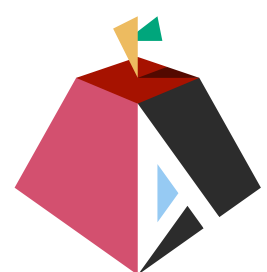
12:34:56:78:9a:bc awd10

LLW traffic

12:34:56:78:9a:bc llw0



→ Submission Ring (H2D)
← Completion Ring (D2H)



Linux

Receiving Traffic via awd10/11w0

Firmware

AP communication

aa:bb:cc:dd:ee:01 wld0

AWDL traffic

12:34:56:78:9a:bc awd10

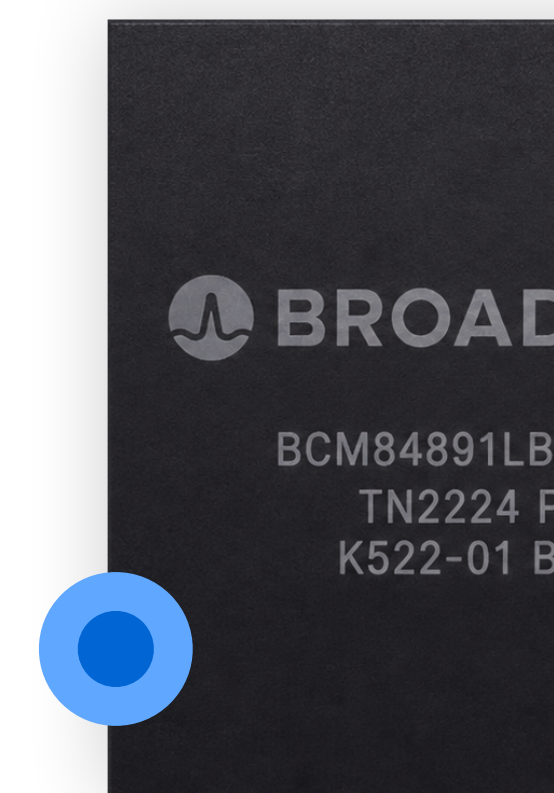
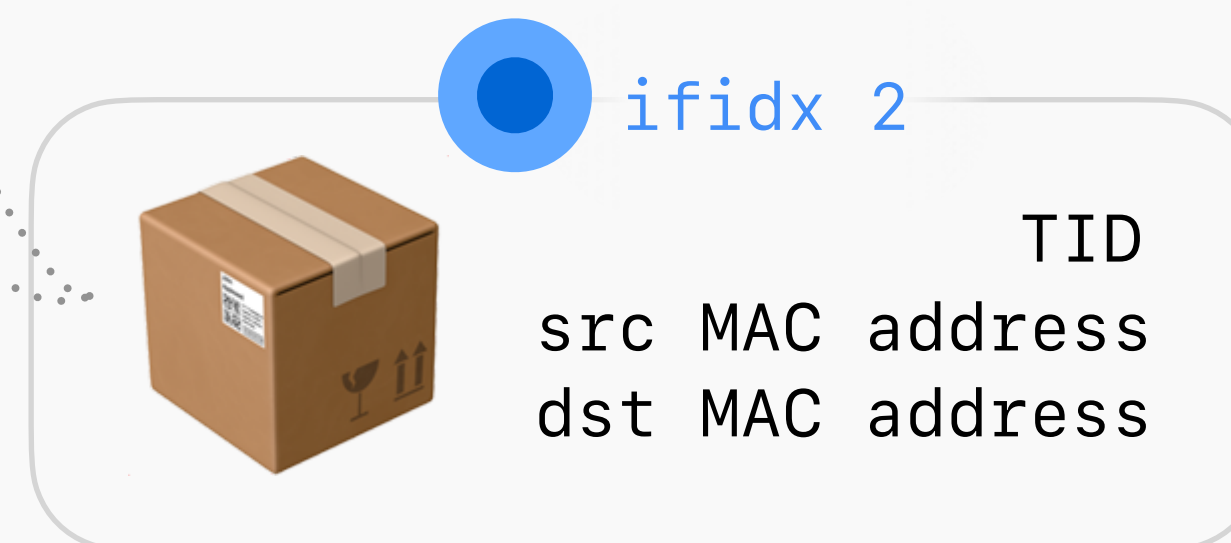
LLW traffic

12:34:56:78:9a:bc llw0

Shared Memory

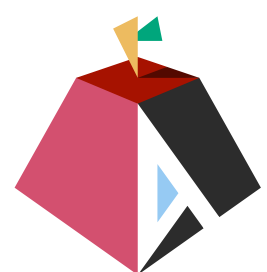


???



→ Submission Ring (H2D)

← Completion Ring (D2H)



Linux

Receiving Traffic via awd10/11w0

Firmware

AP communication

aa:bb:cc:dd:ee:01 wld0

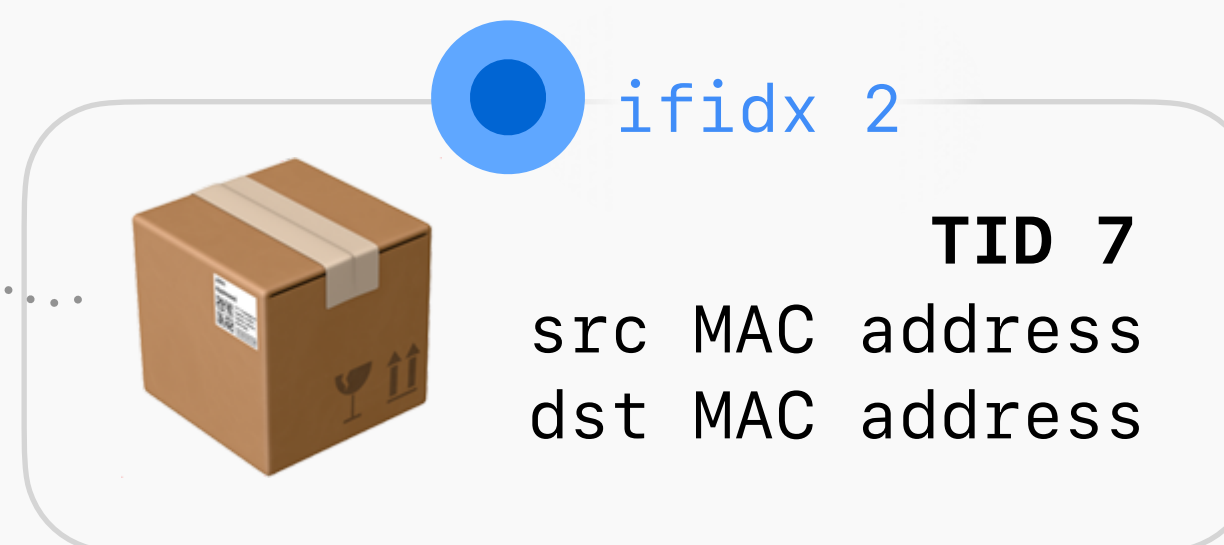
AWDL traffic

12:34:56:78:9a:bc awd10

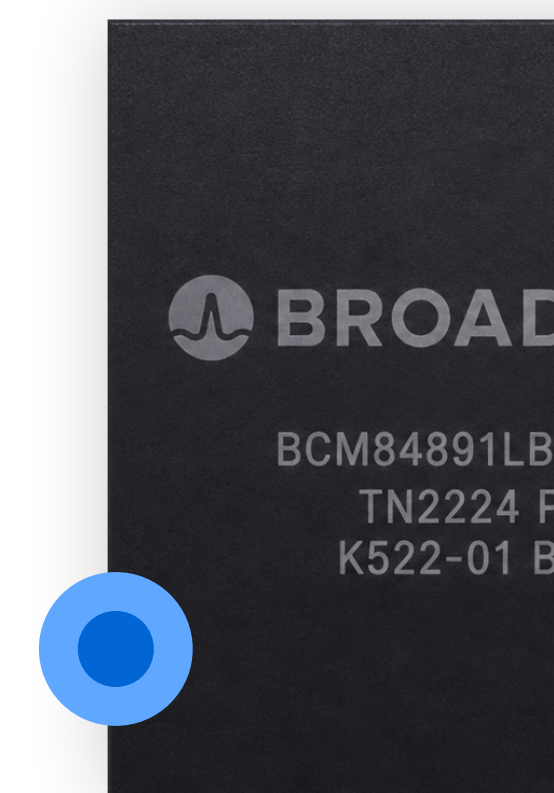
LLW traffic

12:34:56:78:9a:bc llw0

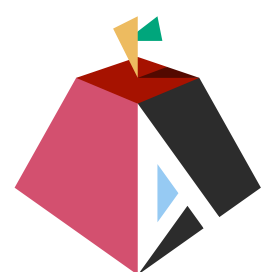
TID 7



Shared Memory



→ Submission Ring (H2D)
← Completion Ring (D2H)



Linux

Receiving Traffic via awd10/11w0

Firmware

AP communication

aa:bb:cc:dd:ee:01 wld0

AWDL traffic

12:34:56:78:9a:bc awd10

LLW traffic

12:34:56:78:9a:bc llw0

other TIDs

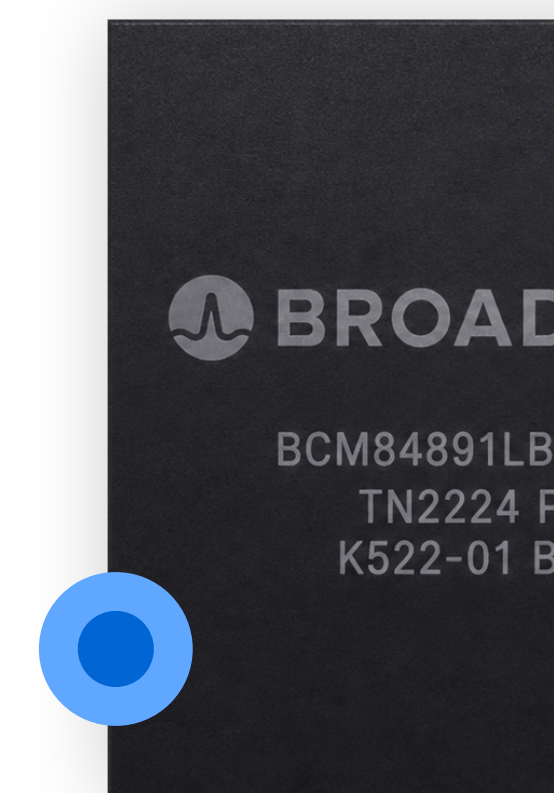
Shared Memory



ifidx 2

TID ≤ 6

src MAC address
dst MAC address



→ Submission Ring (H2D)
← Completion Ring (D2H)

Demo

```
henri-research@fedora-mba-m1-1:~$ ./llw-node listen
```

I

```
henri-research@fedora:~$ ./llw-node demo
```

Where things stand

Working LLW/AWDL unicast and broadcast

Driver-level support on Asahi Linux

What's still ahead

Interoperability with Apple Platforms

Dynamic AWDL/LLW state machine

Support for other Broadcom chips

Funding provided by



Input?

Literature

[A] <https://www.openkritis.de/> (visited 12/09/2026)

[B] <https://media.ccc.de/v/39c3-cracking-open-what-makes-apple-s-low-latency-wifi-so-fast> (visited on 12/09/2026)

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

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

[E] 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 12/09/2026)

[F] 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 12/09/2026)

[G] 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 12/09/2026)

[H] 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 12/09/2026)

Literature

[I] 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 12/09/2026)

[J] 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 12/09/2026)

[K] Shing Tak Yan, Lu Ye, Hongbing Wu, Raghavendra Kulkarni, Edward Myers, Hsieh-Chih Shih, Shadi Saberi, Darshan Kadia, Dizle Ozis, Lei Zhou, Eric Middleton, 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 12/09/2026)

[L] <https://android.googlesource.com/kernel/google-modules/wlan/syna/dhd43752p/+/refs/heads/android-gs-akita-android16-beta-3/include/wlioctl.h> (visited on 12/09/2026)

[M] https://github.com/AsahiLinux/asahi-installer/tree/main/asahi_firmware (visited on 12/09/2026)

[N] <https://blacktop.github.io/ipsw/docs/cli/ipsw/extract/> (visited on 12/09/2026)

Figures

[1] https://de.wikipedia.org/wiki/Universität_Potsdam#/media/Datei:Universität_Potsdam_logo.svg (visited on 12/09/2026)

[2] https://upload.wikimedia.org/wikipedia/commons/thumb/f/f2/Hasso-Plattner-Institut_logo.svg/1920px-Hasso-Plattner-Institut_logo.svg.png (visited on 12/09/2026)

[3] <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 12/09/2026)

[4] <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=WG0zcWo4VEd2YnZ3WTIBVIBwSHNCUnZ0SFIlldzZrSzBMWjRQMnF1U2Y2enZhWUNqTDdqTGdxV2EvMEFJcW1vNDg0SERaYTF4eEZ1aW9ZbGpONkszsXRhaHNubVvXOWRtVW4zMgQxeFF6U00> (visited on 12/09/2026)

[5] https://upload.wikimedia.org/wikipedia/commons/thumb/d/d2/IPad_10.2-inch.png/1280px-IPad_10.2-inch.png (visited on 12/09/2026)

[6] https://cdsassets.apple.com/live/SZLF0YNV/images/sp/111911_sp807-ipad-7th-gen.png (visited on 12/09/2026)

[7] https://drive.google.com/file/d/1QvLTWECNhQpd10IIW1nz8nUTKvFup_jk/view (visited on 12/09/2026)

[8] https://store.storeimages.cdn-apple.com/1/as-images.apple.com/is/MXK53_AV1?wid=1144&hei=1144&fmt=jpeg&qlt=90&.v=QytENXB3MzdYRFA4RU1McS9kQ1d6VIZya2IKWIJmUEwrYndWOTJiVWJWQUYwVmtIbGRkS25RMVpBRlo0bk5DUStteWFnS2JDbkxFb1JqRG5KS1RPUWc (visited on 12/09/2026)

Figures

- [9] <https://store.storeimages.cdn-apple.com/1/as-images.apple.com/is/MXCL3D?wid=1144&hei=1144&fmt=jpeg&qlt=90&.v=MWhTMGgwN3h3cm1YQ0hHeIVYWWZ2RExJNzJtbW9WRzBUckZ4SDR0aldyMFY0ZGtxRm5nMGhUUUYyQ1NONFVVUnBSYmQxNkhWTGV4d1BxVjd4aUJPSGc> (visited on 12/09/2026)
- [10] <https://cdsassets.apple.com/live/7WUAS350/images/macros/ventura/macros-ventura-macbook-pro-iphone-13-pro-continuity-camera-desk-view-hero.png> (visited on 12/09/2026)
- [11] 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 12/09/2026)
- [12] https://web.archive.org/web/20240917165129im_/https://cdsassets.apple.com/live/7WUAS350/images/macros/sequoia/macbook-air-13in-iphone-15-pro-macos-sequoia-ios-18-iphone-mirroring-hero.png (visited 12/09/2026)
- [13] <https://image.coolblue.de/max/2048xauto/products/2112531> (visited 12/09/2026)
- [14] https://asahilinux.org/img/AsahiLinux_logo.svg (visited 12/09/2026)
- [15] <https://static.wikia.nocookie.net/ipod/images/8/87/IPSW.png/revision/latest?cb=20210221211146> (visited 12/09/2026)
- [16] <https://static.wikia.nocookie.net/logopedia/images/d/de/Macos-ventura.png/revision/latest/scale-to-width-down/1000?cb=20230719194655> (visited 12/09/2026)
- [17] <https://nl.net.nl/logo/banner-bw.svg> (visited 12/09/2026)