Mission Critical Communication Services over Wi-Fi

Mark Grayson
Cisco Fellow

May 2026

Agenda

1. Why a focus on Mission Critical Services?
2. Components of Mission Critical Services
3. Emergency Calling over Wi-Fi
4. First Responder (NS/EP) Services
5. Emergency Alert Notifications
6. Key Take Aways

1. Why Wi-Fi for Mission Critical Services?

Wi-Fi is the de facto standard for in-building wireless connectivity and is often the only available access in many environments.

IMT 2030 and 6G requirements for deep in-building service continuity are being used to justify more cellular deployments.

Demonstrating Wi-Fi's readiness is critical to ensure it remains part of the solution.

Regulatory codes, such as International Fire Code Section 510, require approved emergency responder radio coverage in all new buildings.

2. Components of Mission Critical Services

Emergency Calling

Ability for a Wi-Fi capable device to make an emergency 911/112 call over Wi-Fi. Credential-less access is sometimes an existing national regulatory requirement.

National Security & Emergency Preparedness

Wi-Fi APs granting prioritized access for NS/EP (e.g., first responders, and other emergency personnel) users during emergency situations.

Emergency Warning Systems

A system that delivers emergency alerts such as tsunami warnings, earthquake notifications, or AMBER alerts to Wi-Fi users.

Built on a foundation of secure and seamless guest access, using Passpoint and OpenRoaming

2. WBA Driving Mission Critical Industry Programs

Emergency Calling

National Security & Emergency Preparedness

Emergency Warning Systems

Built on a foundation of secure and seamless guest access, using Passpoint and OpenRoaming

3. Emergency Calling

80% of all E911 calls are made over wireless

80% of all data is consumed indoors

20% of all carrier-provided wireless voice calls are made using Wi-Fi Calling

FCC CSRIC VIII recommends extending 911 to Wi-Fi

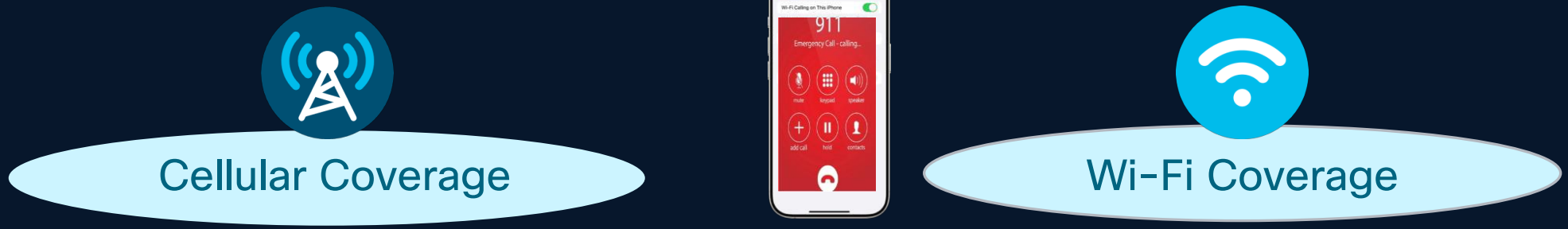
3. Emergency Calling over Wi-Fi: The End Goal

A Wi-Fi capable mobile device in a Wi-Fi only environment is able to place an emergency call using native dialer.

Device seamlessly and securely authenticated to Wi-Fi access network

Device location is available to route the call to the correct Public Safety Answering Point

Dispatchable Location is available when making an emergency call over the Wi-Fi network



3. Wi-Fi 911 Caller Location

- Location-based routing determination functionality is necessary to decide how to route emergency requests towards the correct Public Safety Answering Point (PSAP)
- Once routed to the correct PSAP, location information is again necessary for PSAP operations to determine a dispatchable location to be able to serve the emergency user.
- There is considerable misunderstandings when it relates to using Wi-Fi networks to make emergency calls.
- Much of this is rooted in earlier phone user interface settings that required the user to register an “emergency address” to “help emergency response services respond to calls”.

3. Reporting location of Wi-Fi access

RADIUS LOCATION RFC 5580

RADIUS Protocol
  Access-Request (1)
  Called-Station-Id = "88-15-44-50-0F-1C"
  AVP: t=Location-Information(127), val=0x00016a0312bc6a0313e80000012c4d616e75616c
  AVP: t=Location-Data(128), val=0x00016a0312bc6a0313e80000012c4d616e75616c
Location-Data:
  > Country: "US"
  > CAType: 01 (State), CAValue: "California"
  > CAType: 03 (City), CAValue: "San Jose"
  > CAType: 24 (Postal), CAvalue: "95135"

SIP Private Access Network ID, RFC 7315

REGISTER sip:example.com SIP/2.0
From: <sip:user@example.com>;tag=12345
To: <sip:user@example.com>
Call-ID: 98765@192.168.0.1
Cseq: 1 REGISTER
Contact: <sip:user@192.168.0.1>
Max-Forwards: 70
P-Access-Network-Info:IEEE-802.11ac;i-wlan-node-id=881544500f1c

3. Cellular: historical use of Sector-ID routing

- The Alliance for Telecommunications Industry Solutions (ATIS) estimated that on average 12% of wireless legacy E911 voice calls nationwide, routed on tower-ID were misrouted
- Experiencing along PSAP boundaries was even worse, sometimes as high as 20-50% mis-routing.
- Industry has transitioned to Device Based Hybrid/Advanced Mobile Location for determining emergency call location.
- Totally transparent to the user, with guard rails around location privacy

3. Transition from Network-provided Location to Device-provided

- Device Based Hybris/Advanced Mobile Location Estimates emergency caller's location using cell towers and on-device data sources like GPS and Wi-Fi Access Points.
  1. 2018: Android introduces Emergency Location Service (ELS) delivers DBH location to carriers in USA.
  2. 2017-18: Hybridized Emergency Location (HELO) delivers DBH location to carriers in USA.
  3. 2018: DBH delivered direct to PSAPs through RapidSOS integration, bypassing traditional carrier-to-dispatcher relay
- DBH can be transported using different technologies, according to national requirements:
  - SMS, HTTPS, SIP

3. Device Based Hybrid Transport

SMS

A"ML=1;lt=+51.453520;lg=-0.165978;rd=29.558122;lc=95;top=20260401100000;ei=353586942964984;mcc=234;mnc=15;pm=W

HTTPS

V=1&device_number=%2B4474775931102&location_latitude=55.85732&location_longitude=-4.26325&location_time=1476189444435&location_accuracy=20.4&location_source=GPS&location_confidence=95&location_altitude=0.0&device_imei=354773072099116&device_imsi=262019176307582&ce11 home mcc=262&cell_home_mnc=01&cell_network_mcc=262&cell_network_mnc=01

SIP

```
<gp: geopriv>
  <gp: location-info>
    <gs: Circle srsName="urn:
ogc: def: crs: EPSG:: 4326">
      <gml: pos> 42.93156 -
78.89237</gml: pos>
      <gs: radius>33.150337
      </gs: radius>
    </gs: Circle>
    <con: confidence>95
    </con: confidence>
  </gp: location-info>
  <gp: method>DBH_HELO
  </gp: method>
</gp: geopriv>
```

3. HTTPS DBH to PSAP via Intermediary

On 911 dial, the device OS triggers a silent HTTPS POST carrying HELO or ELS location to the RapidSOS Emergency API. This transmission is asynchronous to and independent of the SIP/IMS voice call path.

iOS HELO; HTTPS Post · TLS 1.2+ ; Enhanced Emergency Data (EED)

Android ELS; HTTPS; TLS 1.2+; Advanced Mobile Location (AM)L Protocol

HTTPS

RAPDSOS (clearinghouse)

Supplementary Location

PSAP (non-i3-compliant)

E911 Center integration – supplements ALI screen

3. Removing the reliance on registered location (and GPS)

- FCC: The broad availability of DBH location technologies combined with the deployment of location-based routing has led to improvements in location information for 911 over Wi-Fi over supporting networks, reducing the reliance upon a user-inputted Registered Location and associated challenges

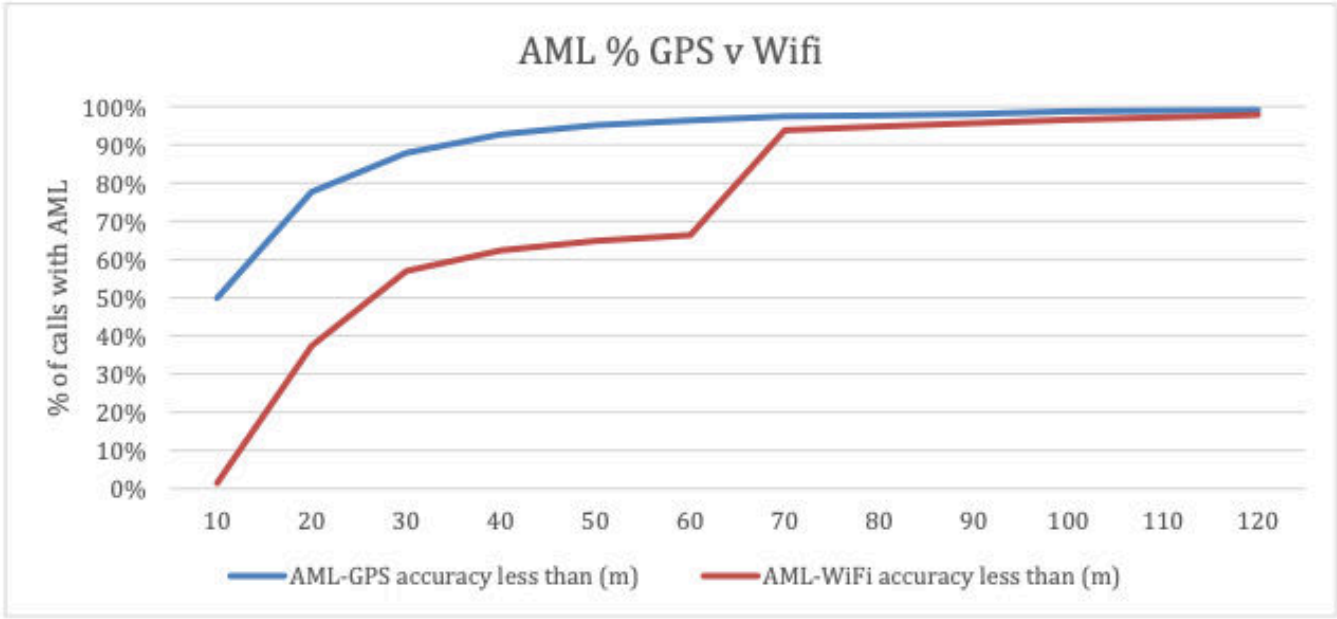
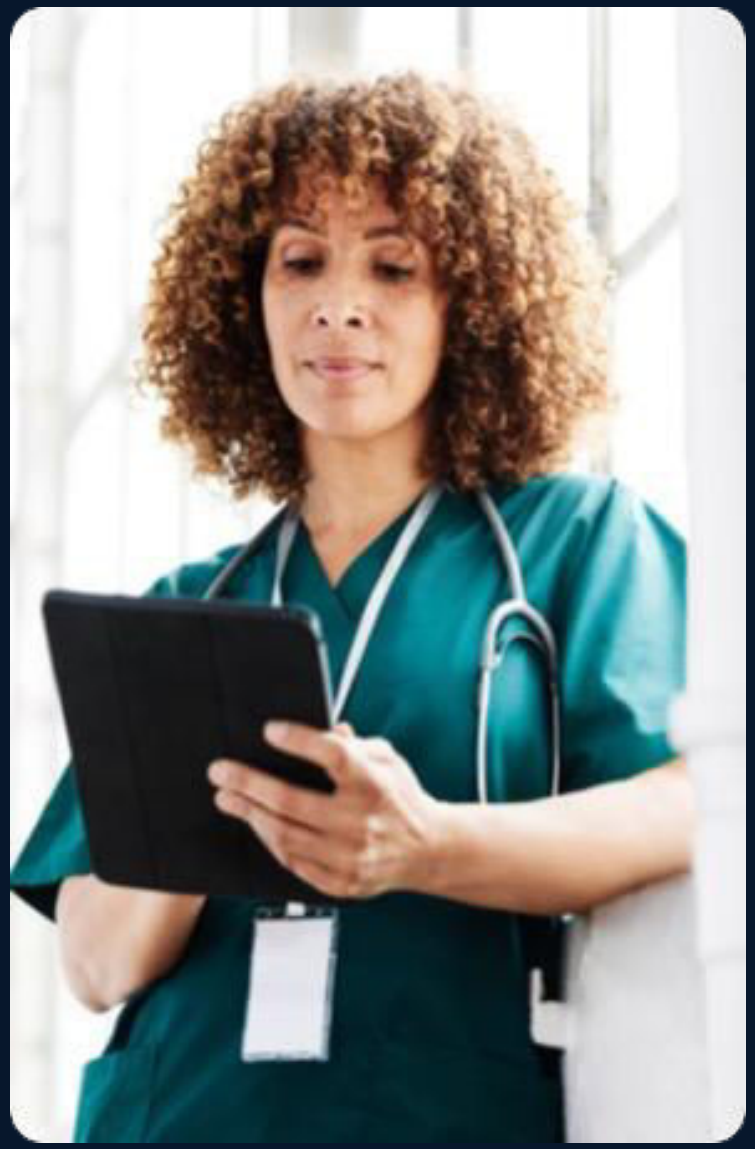


Figure 3 – Cumulative distribution of reported accuracy radii for AML

4. National Security & Emergency Preparedness Services (NS/EP)

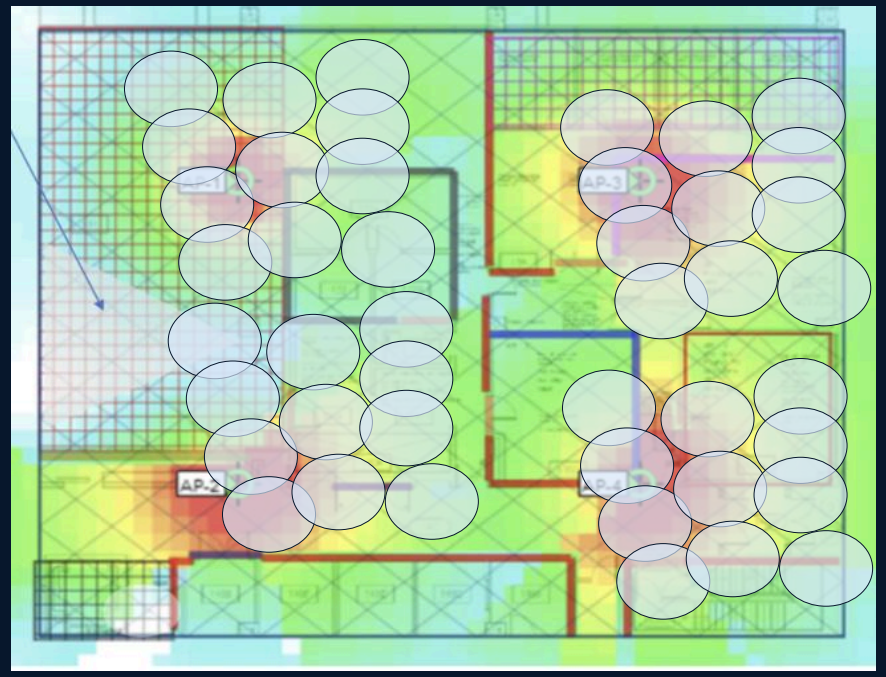
- NS/EP services provide prioritized access to communication networks for first responders, and other emergency personnel during emergencies, ensuring communication during network congestion or outages.
- Communication networks may be congested due to over utilization and ensuring priority access to NS/EP personal is a key regulatory requirement.
  - Cellular networks can implement access class barring to ensure emergency services can continue to access during congestion (AC14 for Emergency Services)
- Carriers receive NS/EP authorization from Cybersecurity and Infrastructure Security Agency (CISA).



4. Mapping indoor cellular RF coverage: From the client's perspective

- Heavy investment in cellular-based emergency responder services
  - While switching from 400 MHz PMR to 800 MHz LTE
- 10% of floor area lacks voice; 33% lacks mobile data (device-reported)
  - 802.11 MBO allows APs to learn about these gaps from devices
- First responders need rich media and multimedia sharing
- Challenge: Ensuring access to next-gen applications throughout all buildings

Cellular dead spots

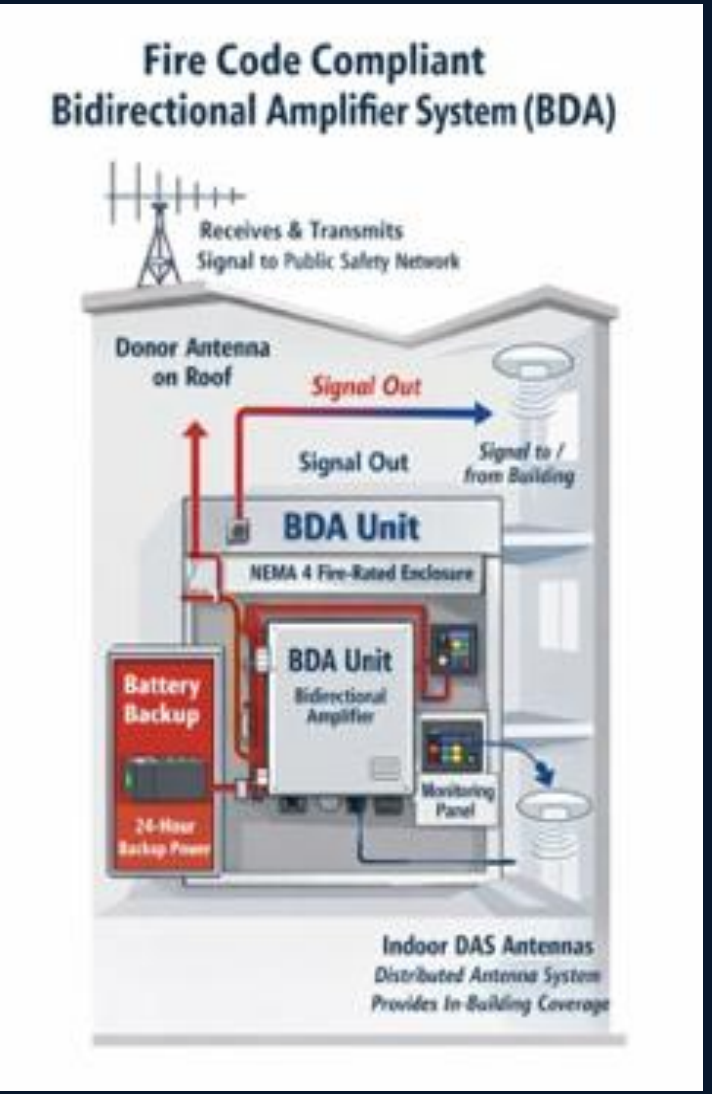


Based on Client Provided Data:

The heatmap is derived using Wi-Fi Alliance Multiband Operations (MBO)standards. The AP actively queries connected clients using 802.11k action frames. The clients "self-report" their cellular experience back to the network. This crowdsourced telemetry is then used for mapping to visualize "dead zones" from the actual device's perspective.

4. Emergency Responder Enhancement System

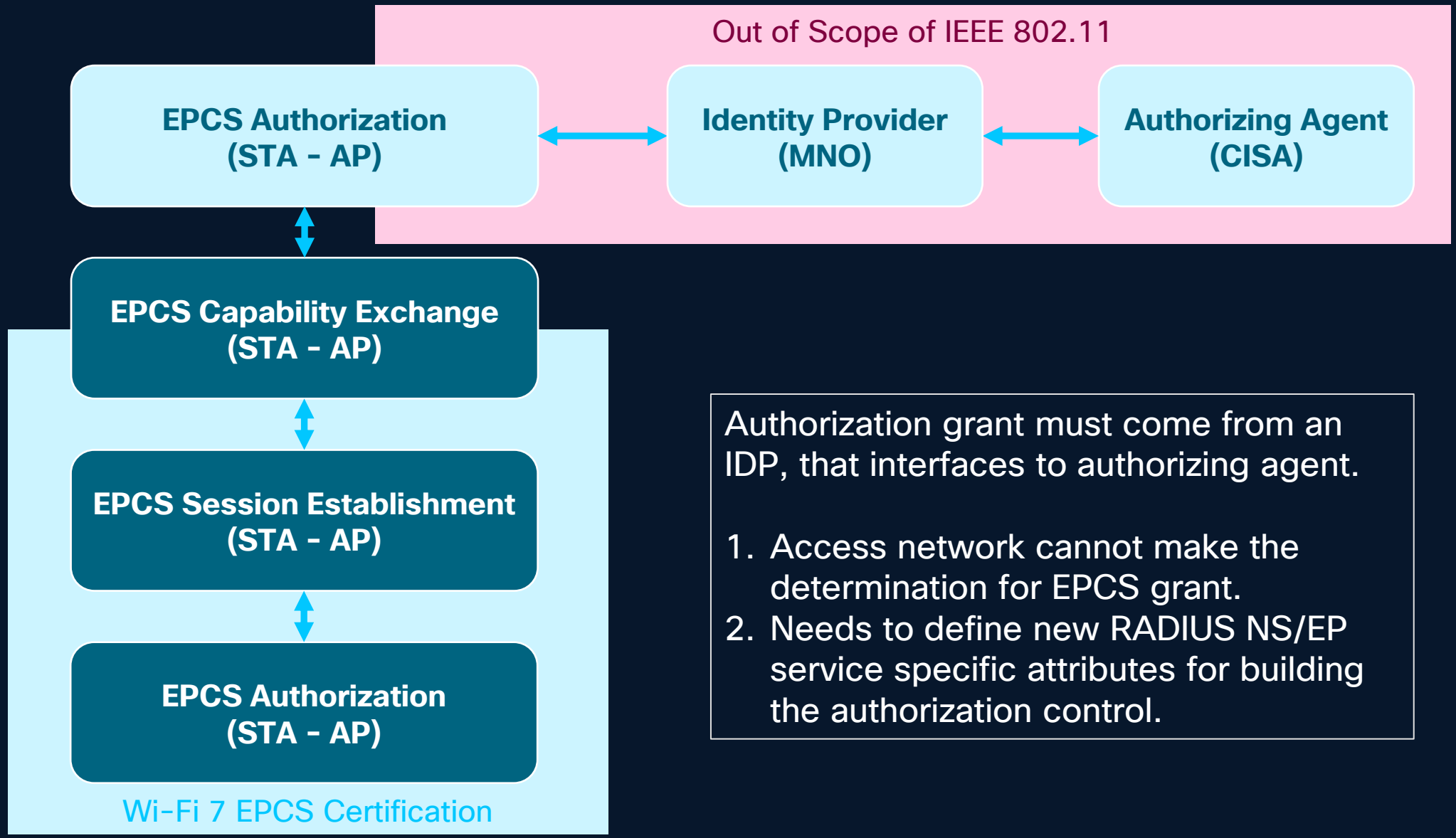
- Occupancy risk and safety determined requirements
- Required when Public Safety Radio System signal level less than -95 dBm in critical areas like stairwells, elevator lobbies and exit passageways
- 12–24 hour battery backups and NEMA 4 waterproof enclosures
- How can public LTE and private Wi-Fi systems complement existing LMR?
- If Wi-Fi is available in areas without LTE or PMR coverage, then how can it be leveraged?



4. Bringing NS/EP Capabilities to Wi-Fi

- While NS/EP services have traditionally been only supported over cellular networks, there is strong interest from federal agencies for enabling NS/EP services over Wi-Fi.
- Wi-Fi 7 includes EPCS (Emergency Preparedness Communications Service) as a feature for providing priority channel access to authorized National Security and Preparedness (NSEP) users.
- There is no WPS roaming in the US
  - All currently deployed roaming systems are unaware of priority-service enablement

4. EPCS Authorization Structure



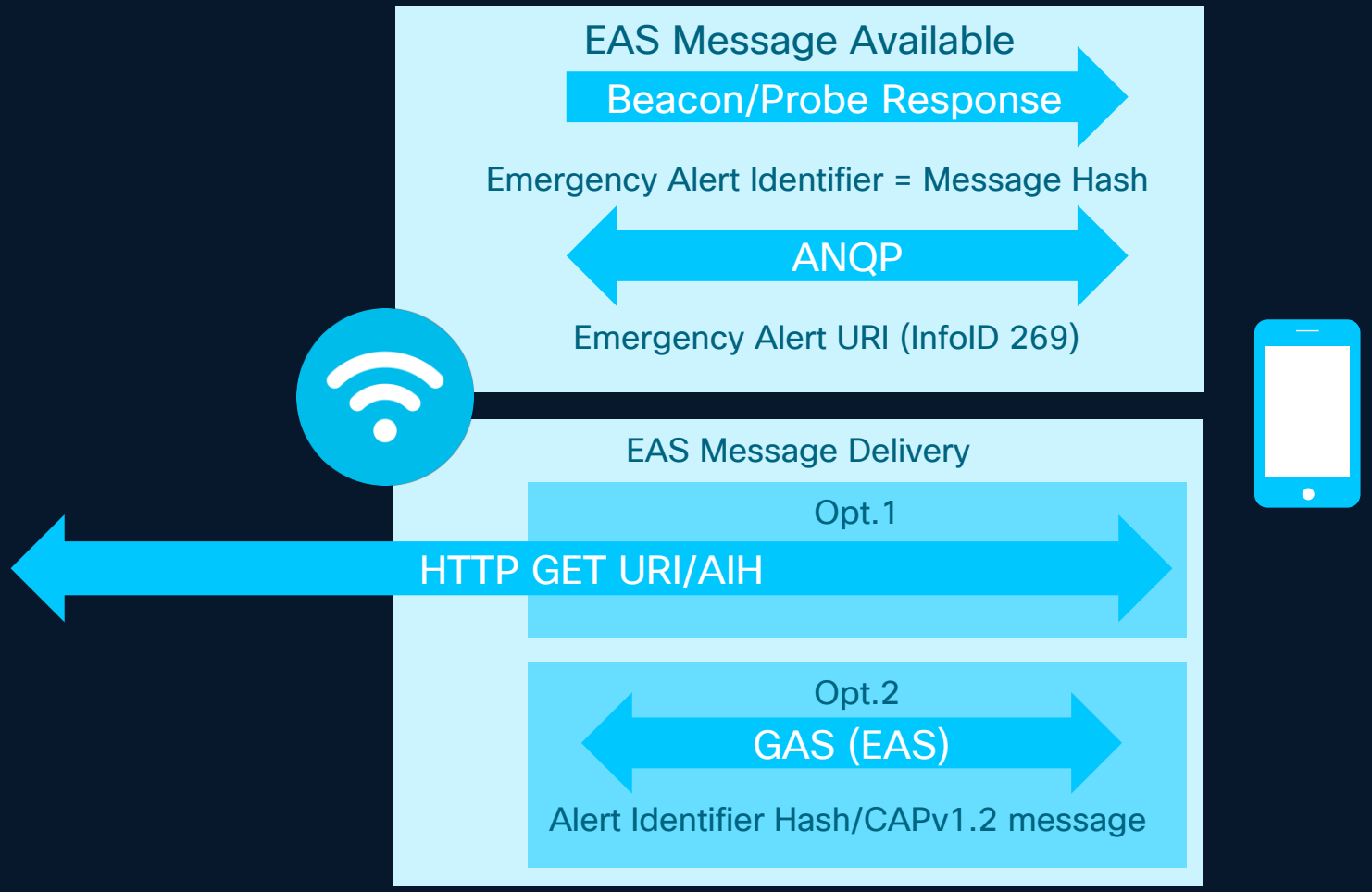
Authorization grant must come from an IDP, that interfaces to authorizing agent.

1. Access network cannot make the determination for EPCS grant.
2. Needs to define new RADIUS NS/EP service specific attributes for building the authorization control.

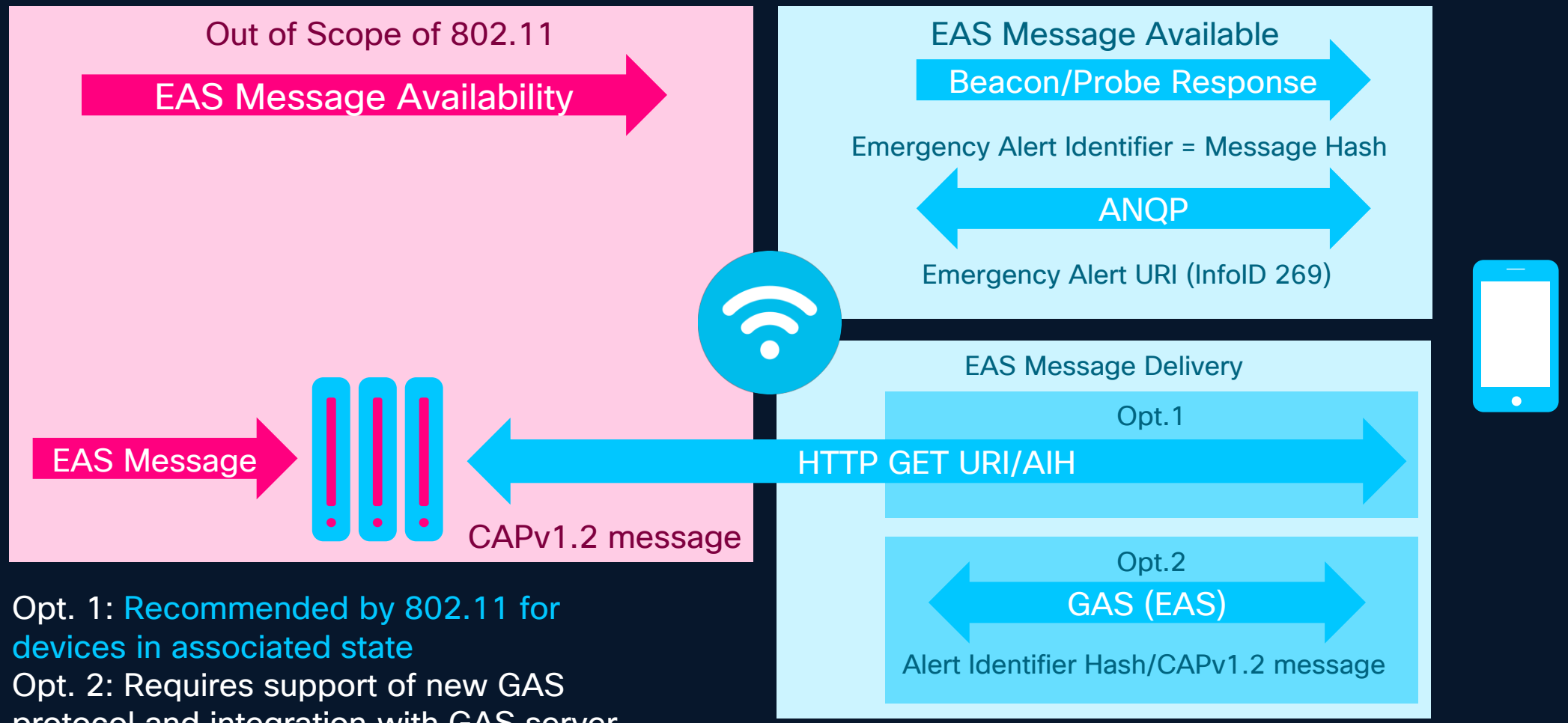
5. Public Warning Messages

- United Nations initiative ensuring that everyone on Earth is protected from hazardous weather, water, or climate events through life-saving early warning systems by the end of 2027
- Not just cellular: “Last-mile communication - All countries ensure the warnings reach those at risk by using multichannel dissemination and communication alerting”
- Ensure messages reach people through preferred and trusted communication channels.

5. IEEE 802.11 Integrated emergency alert system (EAS)

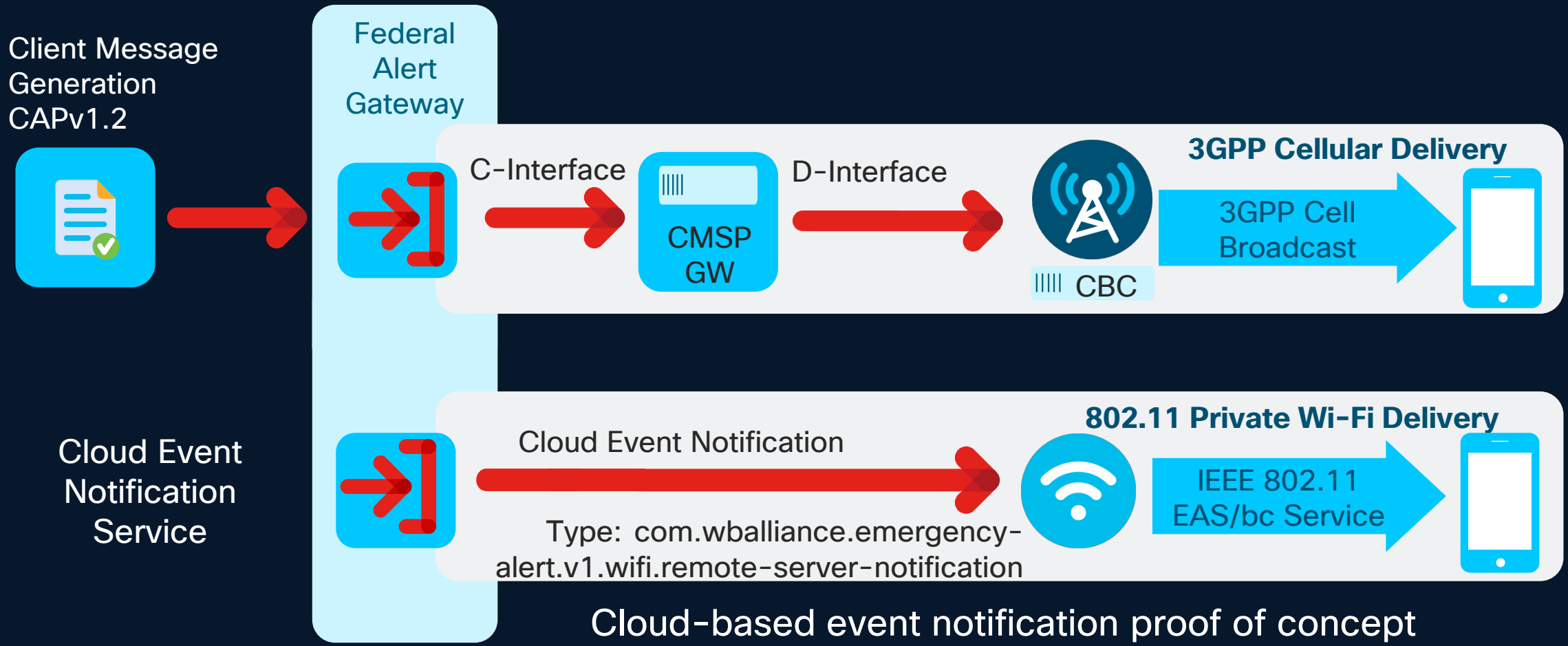


5. IEEE 802.11 Integrated emergency alert system (EAS)



- Opt. 1: Recommended by 802.11 for devices in associated state
- Opt. 2: Requires support of new GAS protocol and integration with GAS server

5. How to scale the delivery of public warning messages?



Cloud-based event notification proof of concept demonstrates that 0.5 Million notifications can be sent to Wi-Fi networks in under 2 seconds

6. Key Take-Aways

Mission-Critical Ready

Wi-Fi now delivers the low-latency, deterministic performance required for emergency calling and public safety.

Precision Location

Transition to DBH and delivery using SIP/PIDF-LO enables location to be used to route and dispatch all emergency calls.

Seamless Access

OpenRoaming eliminates credential barriers, ensuring secure, automatic connectivity for emergency services.

Industry Standards

We are driving WBA standards to ensure these capabilities are interoperable and ready for global enterprise deployment.


CISCO