

**Atea on suurim IT teenuste ja lahenduste pakkuja Põhjamaades ja Baltikumis, tegutsedes Norras, Rootsis, Taanis, Soomes, Leedus, Lätis ja Eestis.**



**1** turuliider  
Põhjamaades



**1** turuliider  
Baltikumis



**84** kontorit



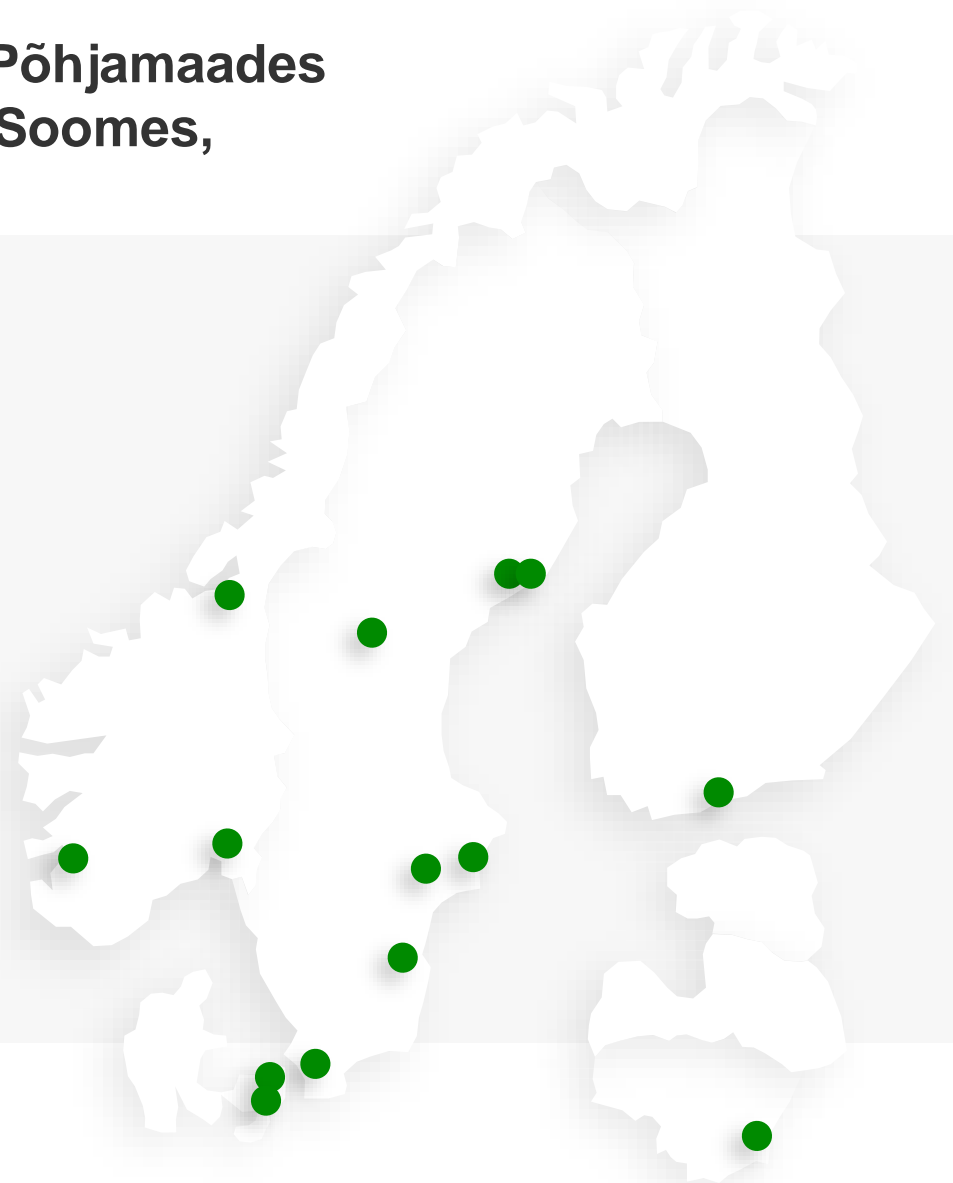
**667** töötajat Balti  
riikides



**128** miljonit eurot  
käive Balti riikides



**4000+** klienti Baltikumis  
era- ja avalikus sektoris



**ATEA**



## Ervi Teearu

IT arhitekt, Atea Eesti



- Cisco CCIE 35497 – 10+ aastat
- Ateas üle 7 aasta
- Panganduses ja telekommunikatsiooni ja IT lahenduste valdkonnas töötamise kogemus
- Cisco lahenduste kogemust 25+ aastat



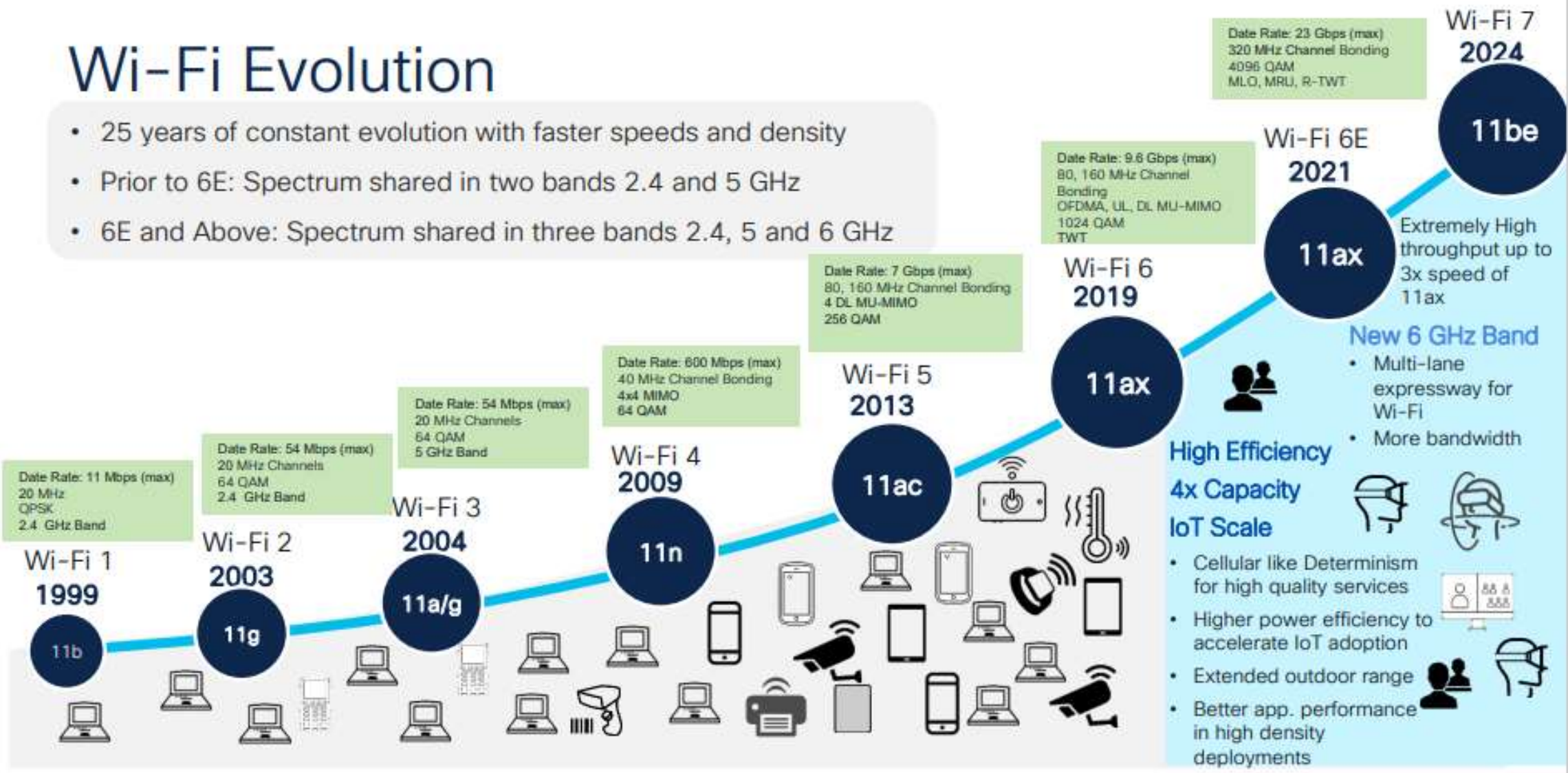
A wide-angle photograph of a modern urban street at dusk. The street is flanked by multi-story apartment buildings with large windows and balconies. The sky is a deep blue, and the buildings are illuminated from within, casting a warm glow. In the foreground, a pedestrian bridge with a metal railing and bollards crosses the street. The overall atmosphere is serene and contemporary.

„WiFi 6E, 7, 8.“

ATEA

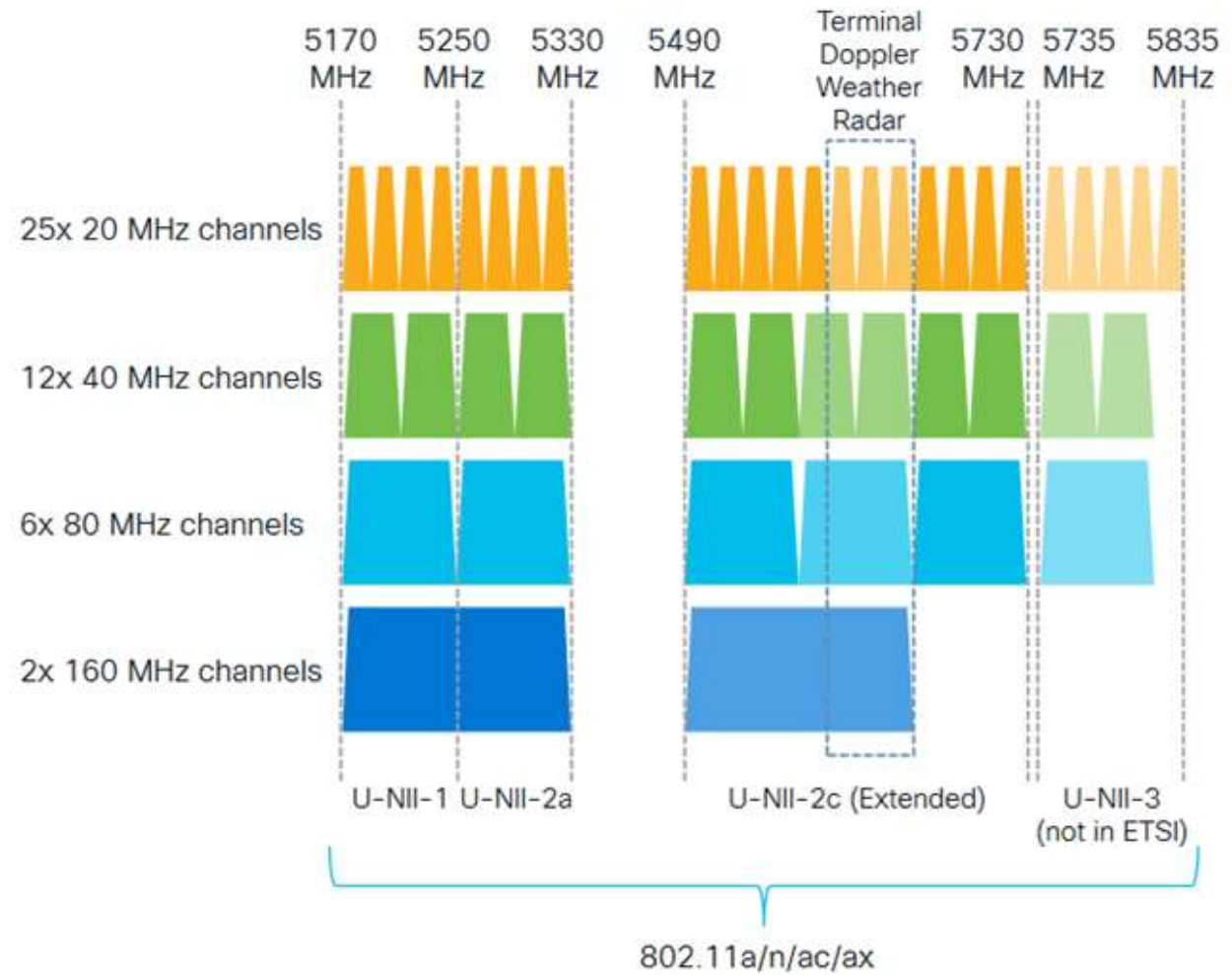
# Wi-Fi Evolution

- 25 years of constant evolution with faster speeds and density
- Prior to 6E: Spectrum shared in two bands 2.4 and 5 GHz
- 6E and Above: Spectrum shared in three bands 2.4, 5 and 6 GHz



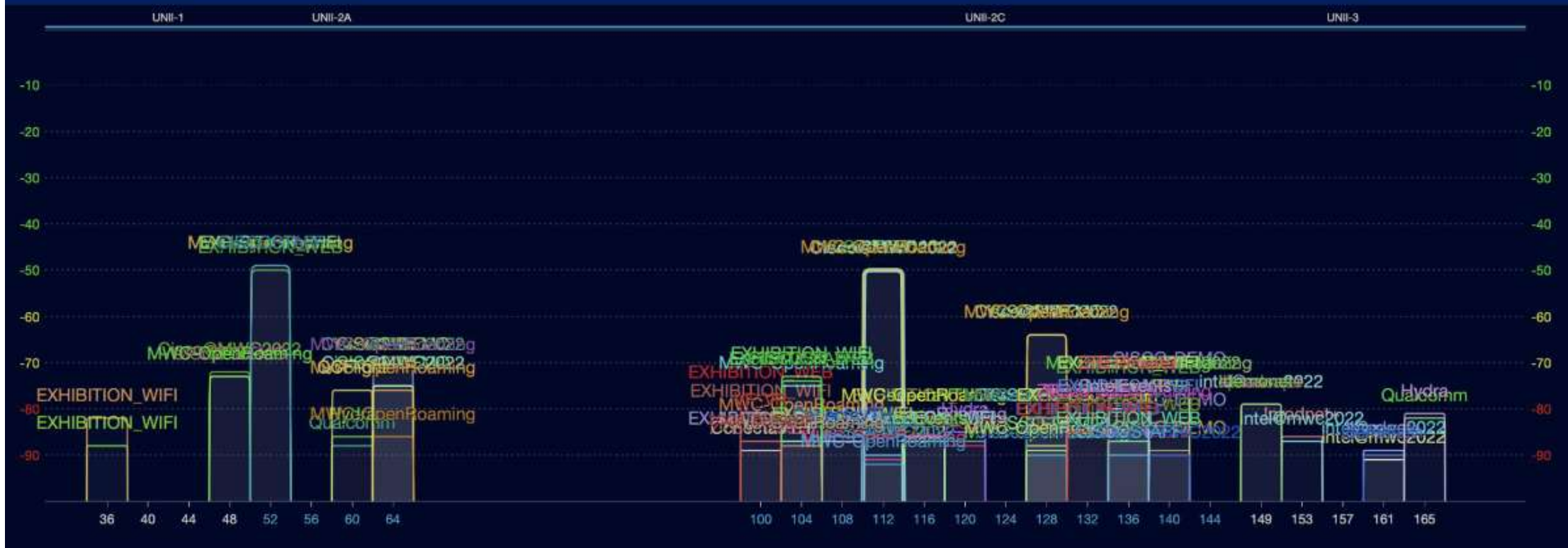
# The 2.4 GHz and 5 GHz bands today

□

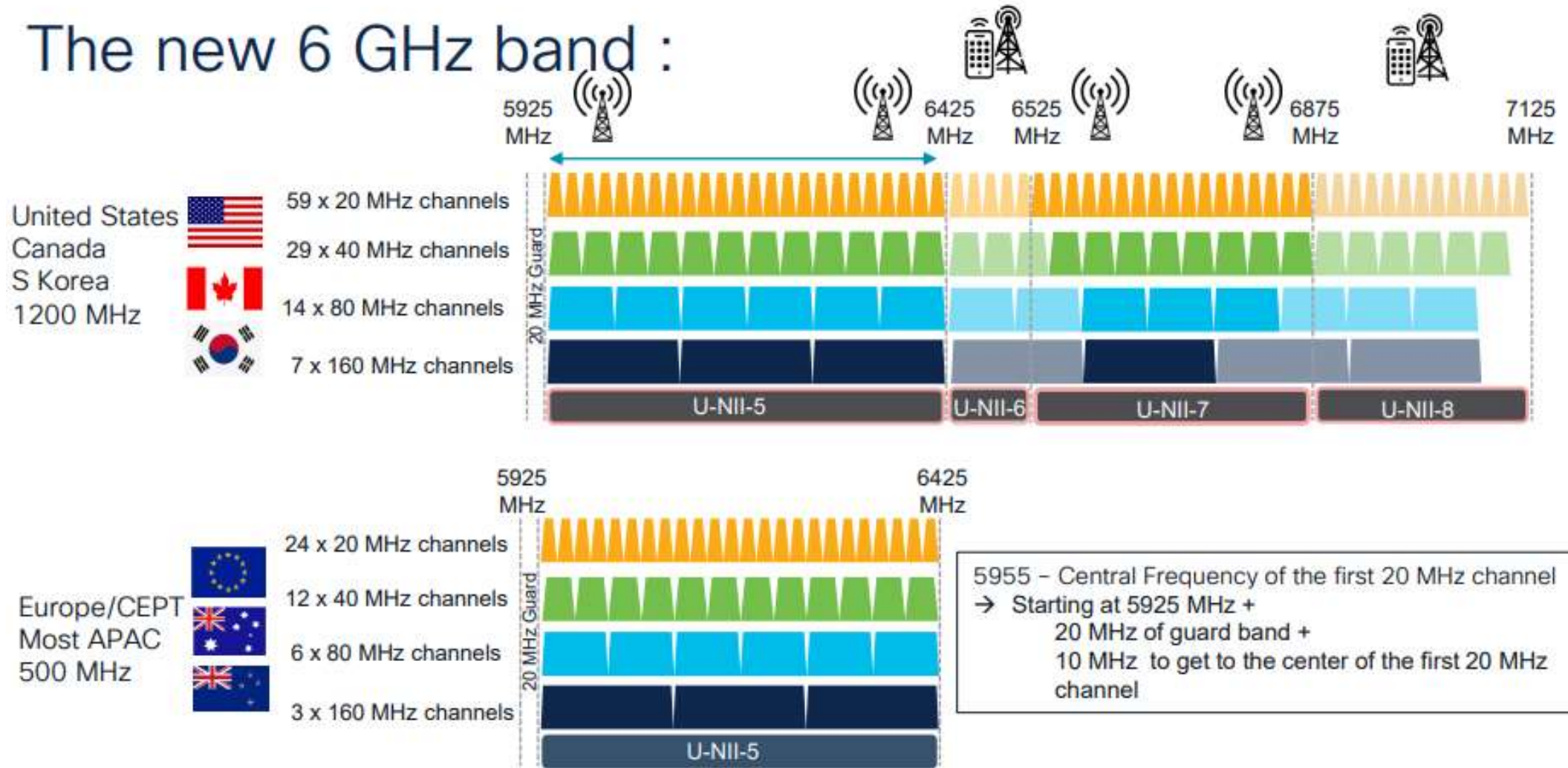


# What is the Problem?

- Existing 2.4 GHz and 5 GHz spectrum is congested
- Legacy clients
- No way to use 80 or 160 MHz channels

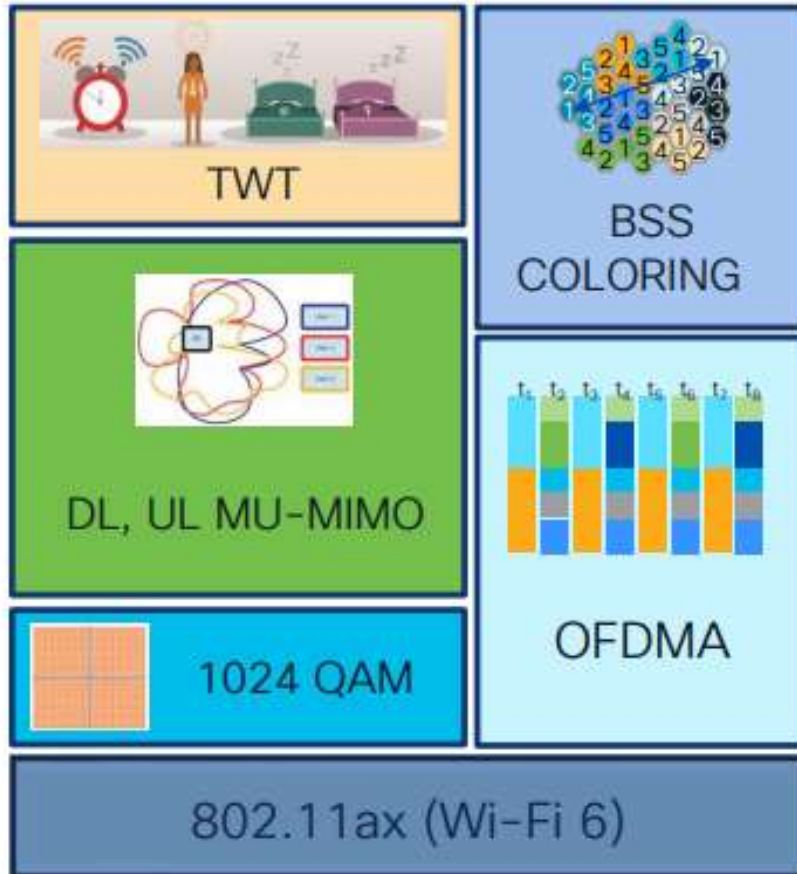


# The new 6 GHz band :



# Wi-Fi 6E

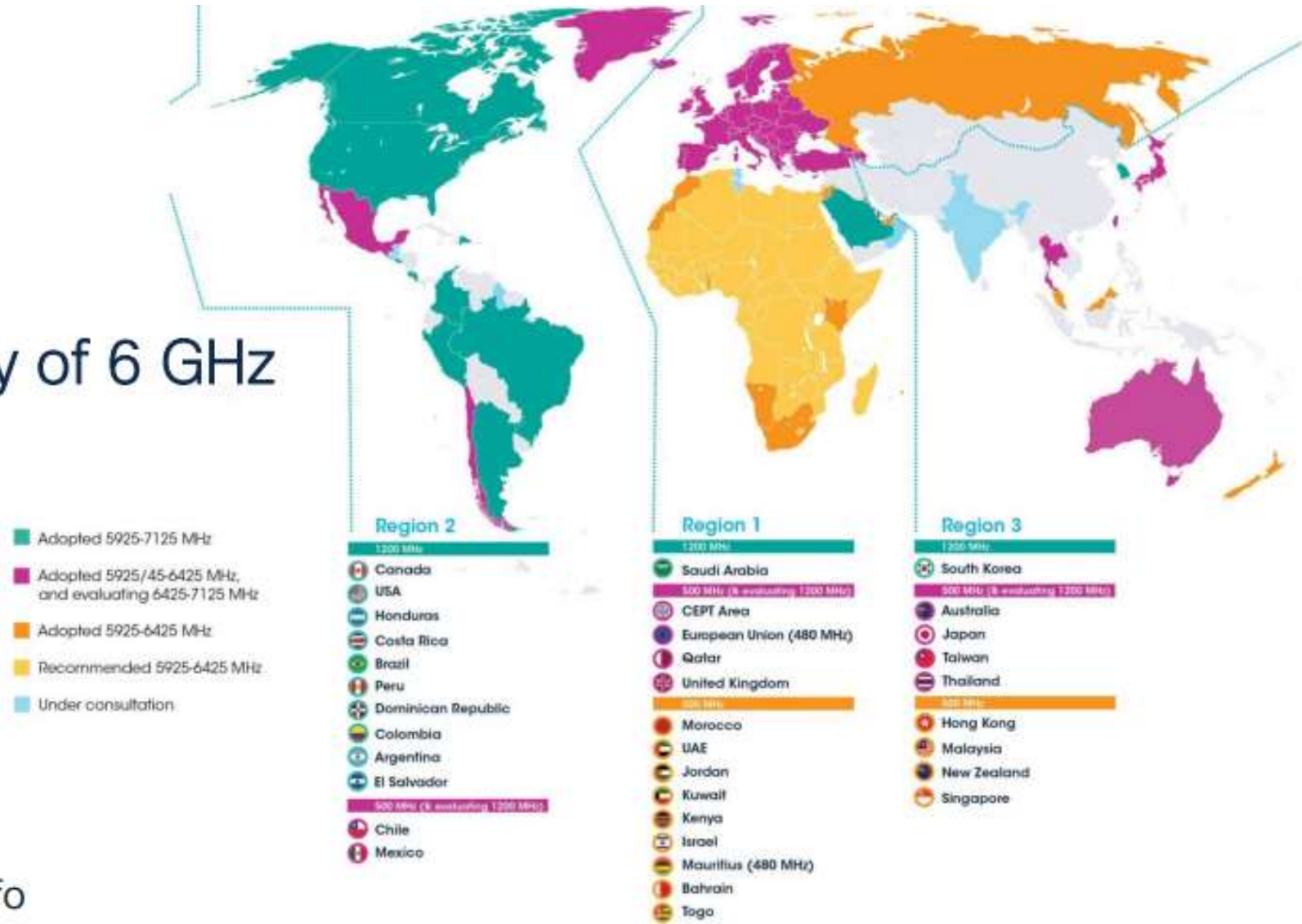
## Wi-Fi 6 and 6GHz are friends!



- 1 Additional Spectrum**  
1200 MHz (5.925 to 7.125 MHz) - US  
500 MHz (5.925 to 6.425) - EU
- 2 Security Upgrade**  
WPA3 Mandatory  
Improves Security
- 3 Clean RF**  
(Fixed Mobile Service Operators in  
UNI-5 and UNI-7)
- 4 No Legacy (Slow) Devices**  
Improves performance
- 5 Protocol Enhancements**  
Airtime Efficiency
- 6 Wider RF Channels**  
80 MHz channels - 1200 MHz  
40 MHz channels - 500 MHz



# Global availability of 6 GHz band for Wi-Fi



Source: <https://6ghz.info>

# Industry's best & broadest Wi-Fi 6E portfolio



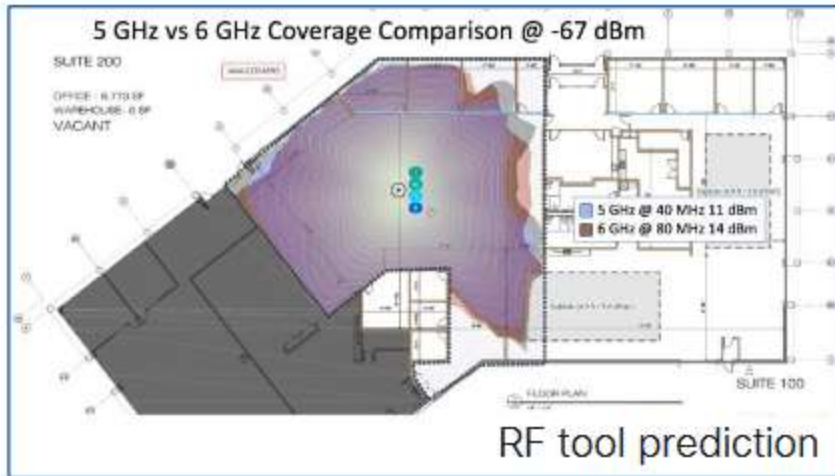
Indoor Access Points

Outdoor Access Point

AT&T

# RF Design considerations

- AP antenna patterns at 6GHz are similar to 5GHz
- **AP coverage** between 5GHz and 6GHz will be similar, especially in open spaces BUT it does require to compensate with **power > 3dB higher in 6GHz**



- 5GHz @40 MHz 11dbm
- 6GHz @80 MHz 14 dbm

- With brick walls, elevator and other environments, you would probably need to measure and add few APs

# Where are we then on 5 and 6 GHz assumptions?

Q1: Can a co-resident 6 GHz radio provide the same coverage as the 5 GHz cell while dramatically increasing performance?

A1: Yes!

Q2: Can a one for one replacement of Wi-Fi 6/5 APs with Wi-Fi 6E APs be achieved?

A2: Yes!

\*Assuming 1.2 – 2k f<sup>2</sup> (140–190 m<sup>2</sup>) of average AP density, carpeted office normal ceiling (3 m / 10 ft)



- 5 GHz network with RRM operating at power levels 3-4? >then equal 5 and 6 GHz coverage is possible with a one for one AP replacement in both ETSI and FCC. Assuming 80 MHz channel in FCC and 40 MHz channel in ETSI/UK
- If the power level is in 1-2, then you may need around 10 to 20% additional access points.

# New Gear!!! Wi-Fi 6E Measurement !

## Ekahau Sidekick 2

- 2.4, 5, 6 GHz
- Ekahau AI Pro
- Ekahau Analyzer



## Hamina Nomad

- 2.4, 5 & 6 GHz
- Hamina Onsite App



## NetAlly Aircheck G3 Pro

- 2.4, 5, 6 GHz
- NetAlly Link-Live



# Wi-Fi 6E Security



Wi-Fi 6E uplevels security.  
WPA3 L2 Security: OWE,  
SAE\*, 802.1x-SHA256



WPA3 and Enhanced Open  
Security made mandatory  
for Wi-Fi 6E certification.



No backward compatibility  
with Open and WPA2  
Security.

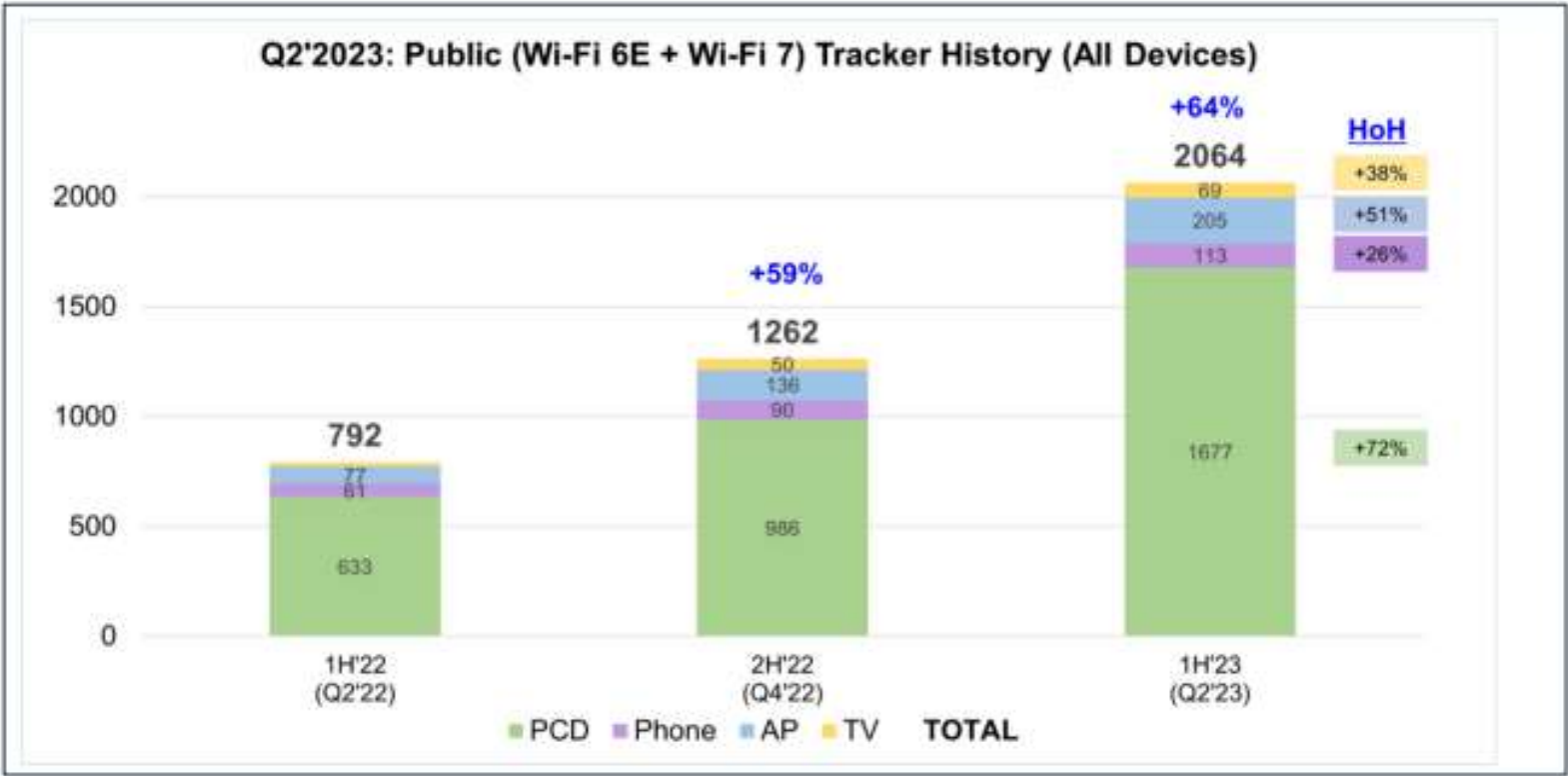


Requires Protected  
Management Frame (PMF)  
in both AP and Clients.

**\*Only SAE-H2E (Hash to Element) Method Supported.  
SAE (Hunting N Pecking) - Not Supported**

AKM = Authentication and Key Management  
OWE = Opportunistic Wireless Encryption  
SAE = Simultaneous Authentication of Equals  
SHA-256 = Secure Hash Algorithm (SHA) 256 bit

# Wi-Fi 6E Device Support



Source: <https://wifinowglobal.com/news-blog/intel-ecosystem-tracking-2064-wi-fi-6e-devices-now-available-wi-fi-7-reaches-67-devices/>



ATERA



# Wi-Fi 7 & 802.11be in 1 slide

Wi-Fi 7 R1 spec finalized in Jan '24. WFA certification for R1 in progress. R2 expected Dec 2025. 802.11be is still not ratified (Exp Dec 2024)

In the enterprise, Wi-Fi 7 is a modest upgrade compared to Wi-Fi 6E. Enterprises can fully utilize the 6GHz spectrum with Wi-Fi 6E

Very few Wi-Fi 7 clients exist, and there is no Wi-Fi 7 support in Windows or MacOS

Cisco has been closely involved in development of Wi-Fi 7, and advocates for thorough client interop testing

6 GHz Wi-Fi with Wi-Fi 6E is mature

# Wi-Fi 7 Security

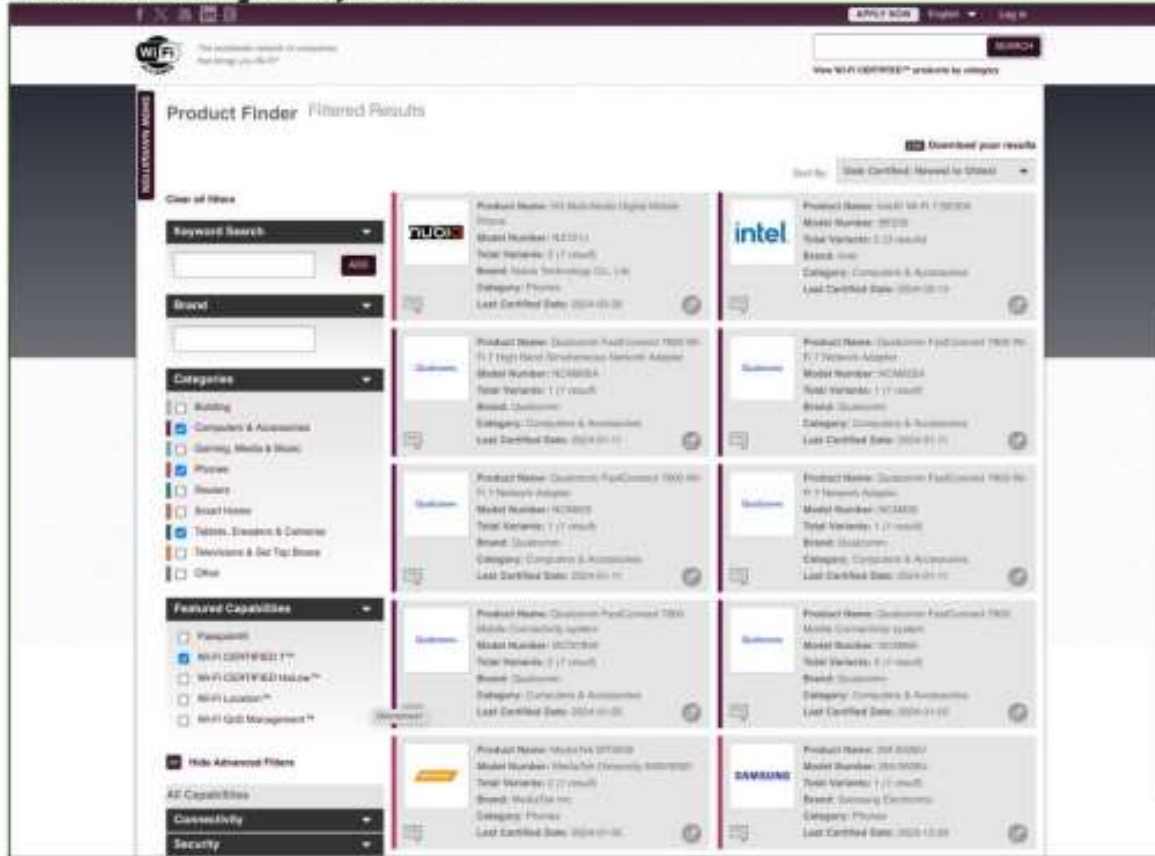
Wi-Fi 7 brings new AKM support for WPA3-SAE and new increased ciphers for OWE & SAE  
 WPA3 /OWE mandatory for EHT (11be MCS rates) & MLO

Older	Wi-Fi 6E (6 GHz)	Wi-Fi 7
Open	OWE (AKM: 18) (Cipher: CCMP 128)	OWE (AKM: 18) (Cipher: CCMP 128 or GCMP 256)
WPA2/WPA3 Transition/ WPA3-SAE(Personal), PMF Optional (WPA 2 - AKM - 2, 4 & 6) (WPA 3 - AKM - 8 & 9) (Cipher: CCMP 128 or AES)	WPA3-SAE (Personal), PMF Mandatory (AKM: 8 & 9) (Cipher: CCMP 128 or AES)	WPA3-SAE (Personal), PMF Mandatory (AKM: 24 & 25) (Cipher: CCMP128 or GCMP 256)
WPA/WPA3 Transition/ WPA3-SAE Enterprise, PMF Optional (AKM 1, 3 & 5, 11 & 12) (Cipher: AES, CCMP 128, GCMP128 GCMP256)	WPA3 Enterprise, PMF Mandatory (AKM: 3, 5, 11 & 12) (Cipher: GCMP 128 & GCMP 256)	WPA3 Enterprise, PMF Mandatory (AKM: 3, 5, 11 & 12) (Cipher: GCMP 128 & GCMP 256)

**Cipher: GCMP 256 – Better Encryption & Speed; AKM: Better security**

# Wi-Fi 7 Certified Client List

As of May 20, 2024

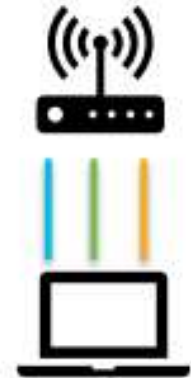


[https://www.wi-fi.org/product-finder/results?sort\\_by=certified&sort\\_order=desc&categories=1,2,3,5,6,7&capabilities=1652&certifications=1275](https://www.wi-fi.org/product-finder/results?sort_by=certified&sort_order=desc&categories=1,2,3,5,6,7&capabilities=1652&certifications=1275)

- **Windows:**
  - Wi-Fi 7 support planned in Windows 11 version in , Second Half of 2024
  - Current support Only in Insider Preview Program (Canary and Dev Channels )
- **MAC:**
  - No support yet.
- **Android:**
  - Support available in Android 13 or greater
- **ChromeBook:**
  - Available 2H, 2024

# On Multilink Operation (MLO)

- Client (STA) connected on multiple bands to the **same** AP, **not** to multiple APs (that is Wi-Fi 8)
- MLO is most likely going to be 2 band on clients – not 3 band
- Single radio client – EMLSR on two links.
- Band-isolation on clients between 5 and 6 determines MLO capabilities; so some clients might “only” do 2.4 + 5, or 2.4 + 6 in MLMR-STR
- Devil is in the detail: Single radio (SR) vs Multi radio (MR). STR vs EMLSR
- Same AKM across all links in an MLO Group (!).



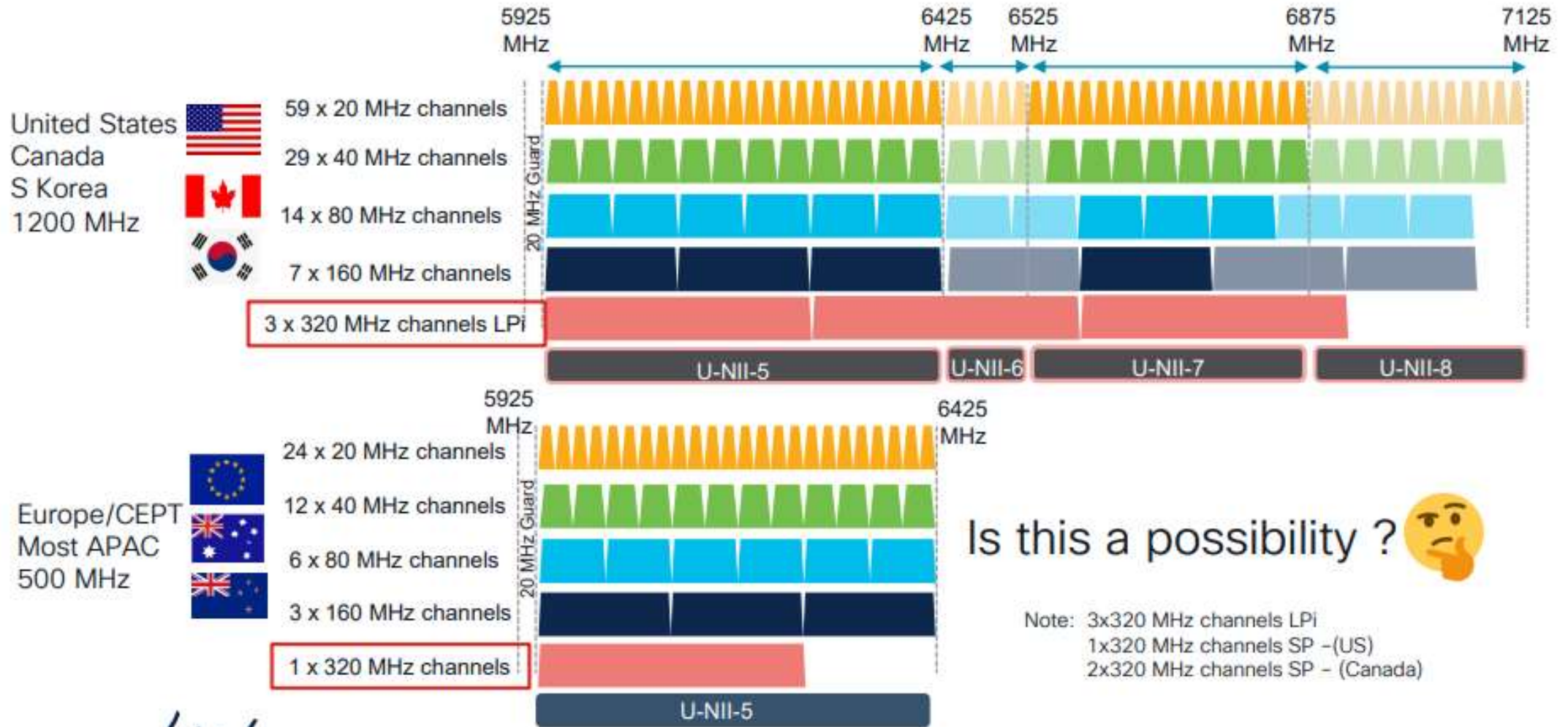
MLO

# 16 Spatial Streams



- Won't be supported in Wi-Fi 7
- Will stay at max 8 spatial streams
- Public docs refer to 16 spatial streams

# Wi-Fi 7 – 320 MHz Channel Width



# 7 Key takeaways:

1. Wi-Fi in 6 GHz is the paradigm shift.
2. Cisco has a full portfolio of products to help customers realize 6 GHz Wi-Fi today.
3. Wi-Fi 7 certification just got available; understand what features are certified.
4. Short to mid-term, Wi-Fi 7 brings only slight benefits in the enterprise vs 6E.
5. Plan for security upgrade. Client interop will be key!
6. Plan for more than 30W per port, and plan for more than 1 Gbps per port.
7. Isn't quite ready for enterprise yet ...





ATEA



# IEEE 802.11bn

Wi-Fi generations <span style="float: right;">V·T·E</span>				
Generation	IEEE standard	Adopted	Maximum link rate (Mb/s)	Radio frequency (GHz)
( <i>Wi-Fi 0*</i> )	802.11	1997	1–2	2.4
( <i>Wi-Fi 1*</i> )	802.11b	1999	1–11	2.4
( <i>Wi-Fi 2*</i> )	802.11a	1999	6–54	5
( <i>Wi-Fi 3*</i> )	802.11g	2003		2.4
Wi-Fi 4	802.11n	2009	6.5–600	2.4, 5
Wi-Fi 5	802.11ac	2013	6.5–6933	5 <sup>[a]</sup>
Wi-Fi 6	802.11ax	2021	0.4–9608 <sup>[1]</sup>	2.4, 5
Wi-Fi 6E				2.4, 5, 6 <sup>[b]</sup>
Wi-Fi 7	802.11be	expected 2024	0.4–23,059	2.4, 5, 6 <sup>[2]</sup>
Wi-Fi 8	<b>802.11bn</b>	expected 2028 <sup>[3]</sup>	100,000 <sup>[4]</sup>	2.4, 5, 6 <sup>[5]</sup>

\**Wi-Fi 0, 1, 2, and 3* are named by retroactive inference. They do not exist in the official nomenclature.<sup>[6][7][8]</sup>

- The goal of 802.11bn is to reach 100 Gbps speeds. This is faster than copper Ethernet which tops out at 40 Gbps. This will require retrofitting ceiling-mounted access points with [single-mode optical fiber](#).
- 802.11bn will require more advanced antennas for channels above 6 GHz which are used in 802.11be and lower. 42.5 GHz and 71 GHz require line of sight and cannot penetrate walls. Outdoors, 802.11bn will be [attenuated by rain](#), as is experienced by [satellite](#) communications.
- Multiple access point (AP) coordination and transmission
- Millimeter wave (mmWave) frequencies
- Low latency

A photograph of a modern city street at dusk. The street is lined with multi-story buildings featuring large windows and balconies. The sky is a deep blue, and the buildings are illuminated from within, creating a warm glow. A pedestrian bridge with a metal railing runs across the street in the foreground. The overall scene is a mix of urban architecture and natural light.

# Cisco Secure Access VPN versus ZTNA

ATEA

# Is VPN Really Dead and Replaced by Zero Trust Network Access (ZTNA)?

## VPN vs ZTNA

VPN	ZTNA
Requires VPN client software	No client software required *
Access to full network or network segment	Access to specific applications
Posture assessed once at VPN authentication	Posture assessed at each application access
1:1 Client-to-Headend relationship	Client can connect to different headends per application

# Cisco Secure Access

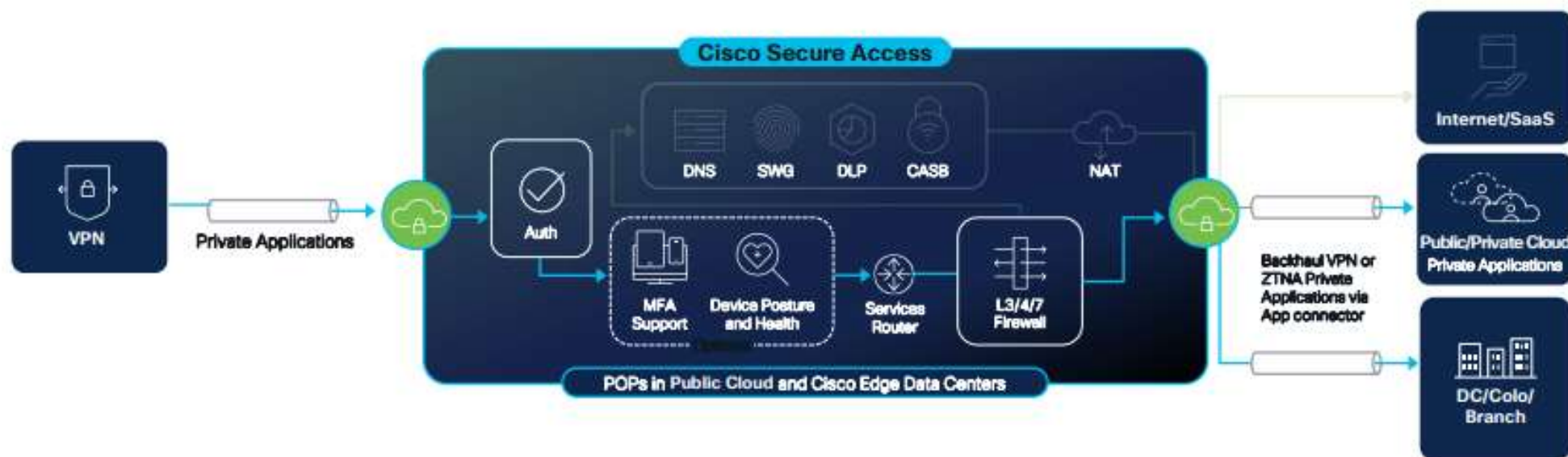
## Capabilities view



# Secure Private Access

via VPN

↔ Private Traffic  
🛡️ Secure Tunnel



## Benefits

- SAML 2.0 + cert-based authentication
- Posture verification (optional)
- Trusted Network Detection
- Start before logon
- IPS
- Granular context-based control

# Cisco Secure Client

- Suite of security service enablement modules



AnyConnect VPN (Core)

ZTA Module

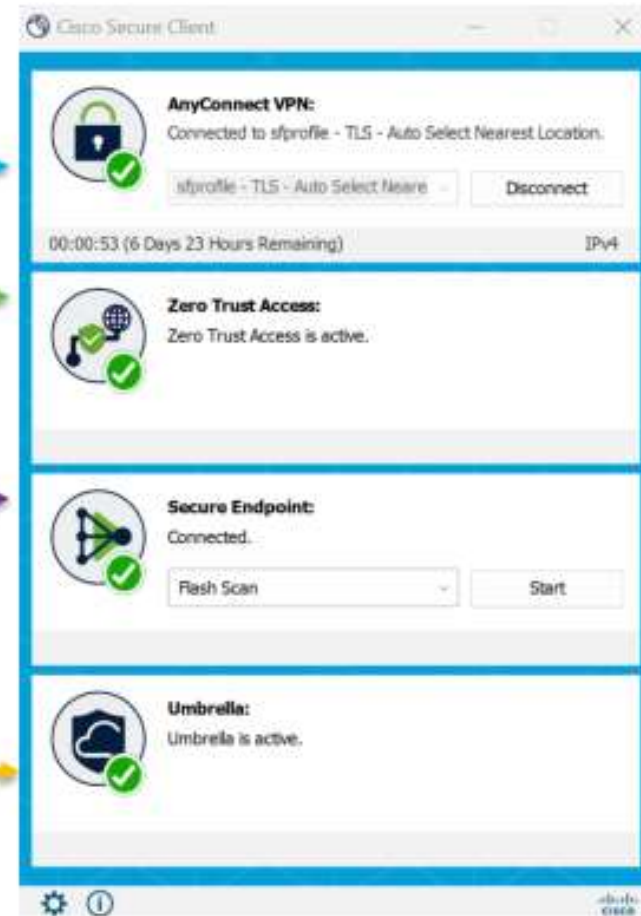
Secure Endpoint (AMP)

Roaming Module

Thousand Eyes (No UI)

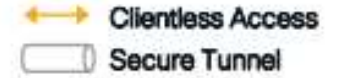
Cloud Management Module (No UI)

Diagnostic and Reporting (DART)



# Secure Private Access

No VPN, No Client



## Capabilities

- Clientless
- App-specific access
- Undiscoverable IP address
- Least privileged user access
- Reduced threat surface

## Key takeaways

- ✓ Both VPN and ZTNA have their strengths and weaknesses. Despite claims of VPN obsolescence.
- ✓ Both technologies can be effectively utilized to establish a secure architecture with Zero Trust Principles.
- ✓ Evaluate and select the most suitable solution for your organization.
- ✓ Contextualize the technologies and consider their implementation based on your organization's specific requirements and objectives.





Kas soovid rohkem teada  
Cisco lahendustest?

---

**Võta meiega  
ühendust:**

[Erv.Tearu@atea.ee](mailto:Erv.Tearu@atea.ee)

**ATEA**