# Overview of IEEE 802.11

*Robert Stacey, Intel*
*Chair, IEEE 802.11*

# IEEE 802.11 Groups

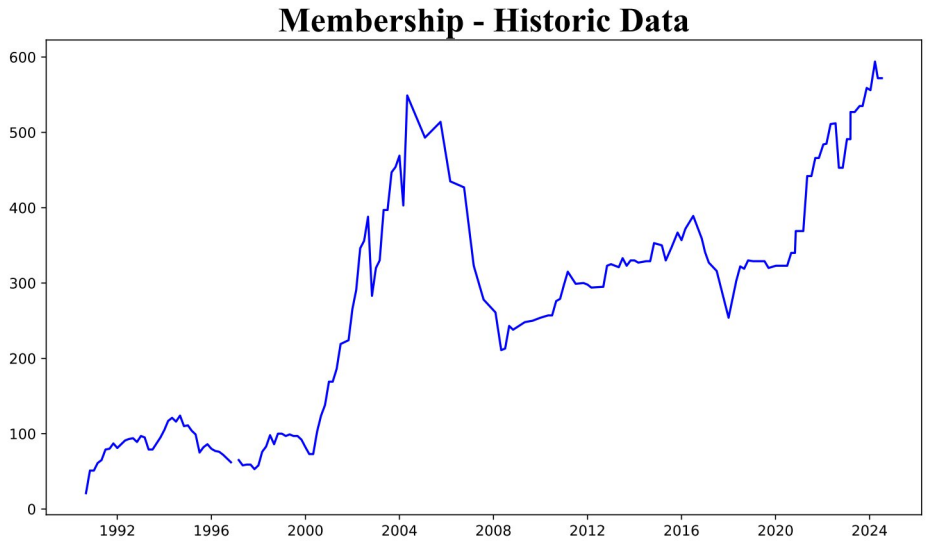
| Type | Group | WG & Infrastructure |
|---|---|---|
| WG | WG11 | The IEEE 802.11 Working Group |
| SC | ARC | Architecture |
| SC | COEX | Coexistence |
| SC | PAR | PAR review |
| 802 SC | JTC1 | ISO/IEC JTC1/SC6 |

| Type | Group | New Work |
|---|---|---|
| SC | WNG | Wireless Next Generation |
| SC | AIML | AI/ML in 802.11 |
| SG | IMMW | Integrated Millimeter Wave |
| AHG | ITU | ITU Liaison |

| Type | Group | Amendments/Revision |
|---|---|---|
| TG | BE | Extremely High Throughput |
| TG | BF | WLAN Sensing |
| TG | BH | Randomized MAC Addresses (RCM) |
| TG | BI | Enhanced Data Privacy Protection (EDP) |
| TG | BK | 320 MHz Positioning |
| TG | BN | Ultra High Reliability |
| TG | BP | Ambient Power |
| TG | ME | Revision (REVme) |

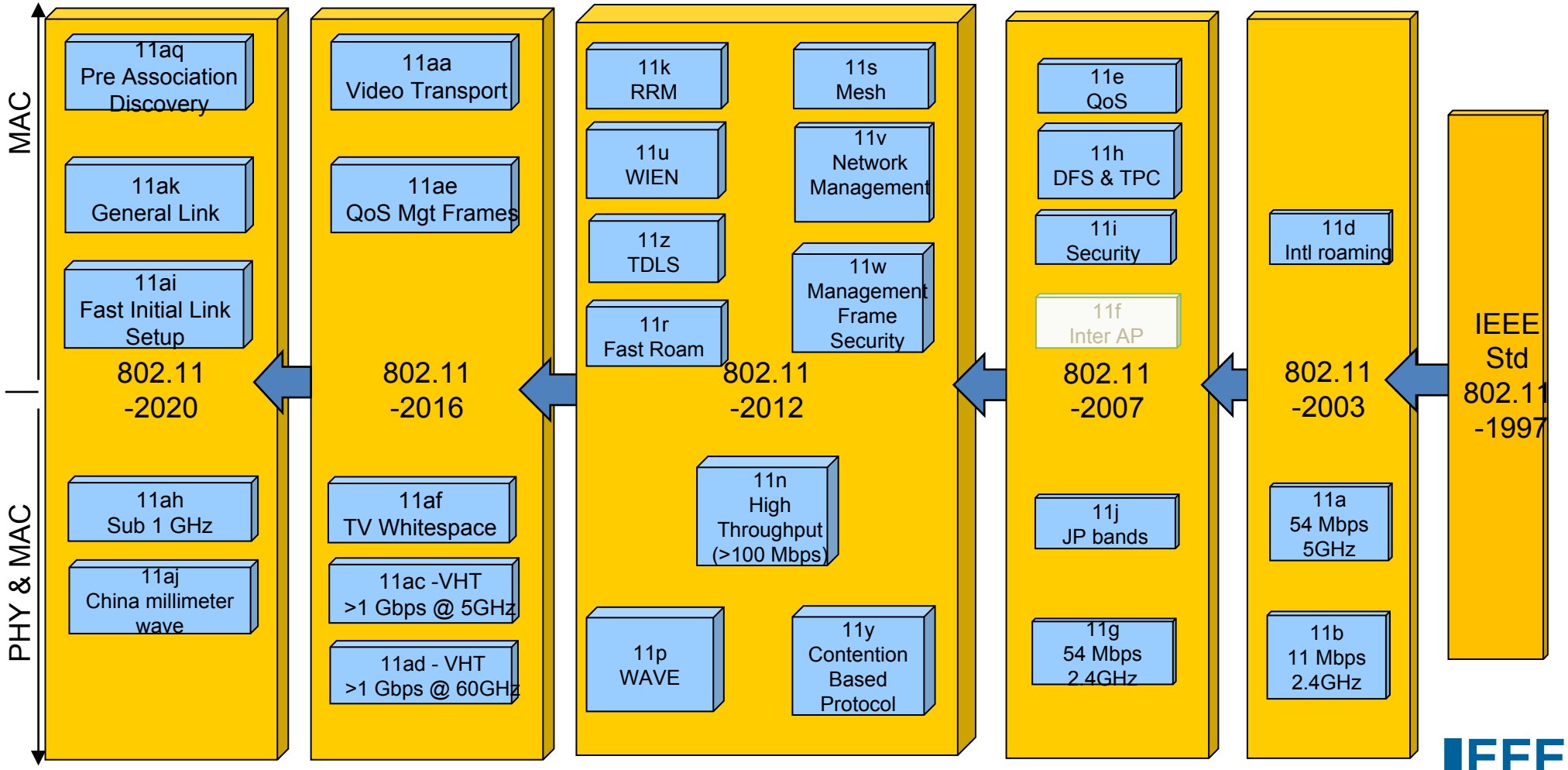
# IEEE 802.11 Membership

| Aspirant | Potential Voter | Voter |
|---|---|---|
| 111 | 64 | 572 |

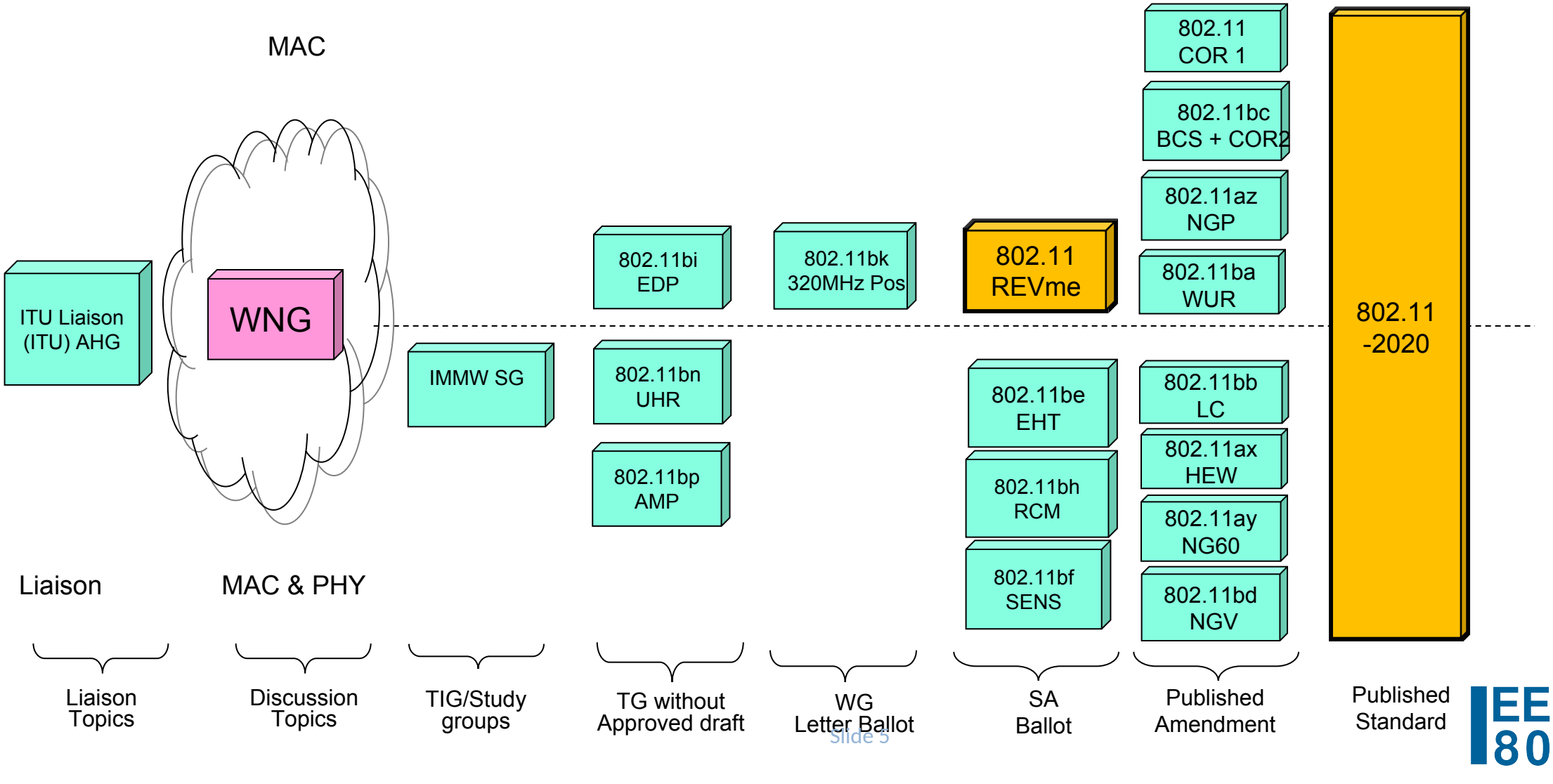



- Membership is at an historic high
- We shifted from in-person to remote attendance during pandemic
- This enabled easy attendance from anywhere in the world
- We now run meetings with both in-person and remote attendance
- Membership is gained by attendance
- Membership is maintained through attendance and ballot participation

# IEEE Std 802.11 Revision History



# IEEE 802.11 Standards Pipeline



# Mainstream evolution

| | Project | Industry Name | Defining features |
|---|---|---|---|
| Completed | 802.11n<br>High Throughput | Wi-Fi 4 | Spatial multiplexing, 40 MHz channels, beamforming, A-MPDU |
| Completed | 802.11ac<br>Very High Throughput | Wi-Fi 5 | 80 MHz & 160 MHz channels, beamforming that works<br>Enabled broad support for 5 GHz band operation |
| Completed | 802.11ax<br>High Efficiency | Wi-Fi 6 and 6E | Multi-user operation, 320 MHz channels, 6 GHz band operation |
| Nearly Completed | 802.11be<br>Extremely High Throughput | Wi-Fi 7 | Multi-link operation (simultaneous use of multiple channels) |
| New | 802.11bn<br>Ultra-High Reliability | Wi-Fi 8* | Lower latency, longer range, faster handover |

*Expected name; will be decided outside of IEEE 802.11

IEEE 802 ITU

# 802.11bn: Ultra-High Reliability

- Expected to be the basis for Wi-Fi 8
- Currently building their specification framework document (SFD):
  - https://mentor.ieee.org/802.11/dcn/24/11-24-0209-03-00bn-specification-framework-for-tgbn.docx
- Expected improvements:
  - Reduce tail latency
  - Reduce roaming latency by taking advantage of multi-link features
  - Allow access on secondary channel while primary channel is busy
  - AP power save
  - Security enhancements, e.g., Control frame protection
  - Extend range by reducing sensitivity gap between client and AP
  - Multi-AP coordination

# Positioning

- Ranging in the form of Fine Timing Measurement (FTM) was introduced in IEEE Std 802.11-2016
  - Derived from an existing “Timing Measurement” frame exchange that supported clock sync
  - Historically referred to a “REVmc FTM” from the revision project that created it
- Since then, it has been enhanced with IEEE Std 802.11az-2022:
  - Support for wider bandwidths Ⓟ enhanced accuracy
  - Secure LTF Ⓟ prevent position spoofing
- Further enhanced with 802.11bk: adds 320 MHz channel support
- FTM is widely supported in both APs and clients
- Supports numerous use cases, including
  - Geofencing (e.g., limiting access to devices within a building)
  - Indoor navigation
  - Aid regulatory requirements (e.g., 6 GHz band AFC)
- And might help with security/privacy, roaming, link adaptation and similar problems
- Overlaps with and compliments similar solutions in BT and UWB

# Sensing

- 802.11bf is developing a protocol for environmental sensing
- Measurements that can be used to monitor environmental conditions and changes
  - E.g., people movement, number of people present, etc.
- Built on sounding (beamforming) waveforms
- Does not define use of the measurements; just defines the sounding exchange and transfer of channel state information
- These are exchanges involving two or more devices; the industry implements 802.11-based one-sided (radar-like) sounding that does not require standardization

# Privacy and security (1)

- 802.11bh is short term project that addresses the device identification problem arising from the use of random and changing MAC addresses
  - E.g., caching of security credentials, billing, troubleshooting
- Defines two secure methods for device identification:
  - IRM: Client tells the AP what MAC address it will use the next time it engages with the AP
  - Device ID: AP gives the client an identifier to be used the next time the two engage
- Both mechanisms based on sharing information securely (post association) that can be used when the devices next encounter each other

# Privacy and security (2)

- 802.11bi is a longer-term project that will enhance privacy
- For example, preventing
  - Device fingerprinting; identifying a device by the unique information exchanged openly prior to association
  - Spoofing attacks; An AP pretends to be J-Lo's home AP in the hopes that J-Lo's phone will try to associate when J-Lo is in the area, thus giving up her location

# Ambient power communication (AMP)

- 802.11bp is a brand-new task group looking into battery-free and very low power operation
- Very early stages, but the topic-of-interest group (prior to task group) produced this report:
  - https://mentor.ieee.org/802.11/dcn/23/11-23-0436-00-0amp-technical-report-on-support-of-amp-iot-devices-in-wlan.docx

# Integrated mmWave (IMMW)

- Currently a study group; with approval expected to start work as task group in January 2025
- Simplify 60 GHz band operation to reduce implementation cost
- Previous generations (802.11ad/ay/aj) assumed stand alone operation; re-design with multi-band support in mind
- Improvements expected:
  - More architectural reuse from low band PHY
  - Eliminate control PHY by taking advantage of multi-link; e.g., sector sweep beamforming directed through low band channel


IEEE
802


ITU