IEEE 802.11

- Original 10Mbps bus topology Ethernet was designed by Xerox in 1973
- **I**nstitute of **E**lectrical and **E**lectronics **E**ngineers **802** LAN/MAN Project was established in 1985 to set about standardising physical/data link layer issues
- The IEEE 802 project is partially comprised of the following Working Groups:
  - 802.3 – CSMA/CD WG (formal Ethernet standard)
  - 802.4 – Token Bus WG
  - 802.5 – Token Ring WG
  - 802.6 – MAN WG
  - **802.11 – Wireless LAN WG** (estd.1987)
  - 802.15 - Wireless PAN WG (estd.1997)

IEEE 802.11

- 802.11 is further broken down into the following projects, among others:
  - 802.11 **MAC** MAC for WLANs
  - 802.11 **PHY** IR, 2.4GHz FHSS, 2.4GHz DSSS
  - 802.11 **a** 2Mbps PHY
  - 802.11 **b** 11Mbps PHY
  - 802.11 **g** Higher 802.11b speeds
  - 802.11 **i** Enhance 802.11 MAC security
  - 802.11 **5GSC** Globalisation of 5GHz
  - 802.11 **PC** Publicity

IEEE 802.11 Radio Frequencies

- In Ireland the responsibility for regulating telecommunications systems and licensing parts of the radio spectrum is given to the Office of the Director of Telecommunications Regulation (ODTR), which from the 1st December 2002 becomes the Commission for Communications Regulation (COMREG).
- On a Europe-wide basis, extending beyond the EU, harmonisation of frequency allocations is handled by the Conference of European Telecommunications Administrations (CEPT), Electronic Communications Committee(ECC).
- In the U.S. the Federal Commications Commission (FCC) regulates all telcommunications systems.
- Globally the U.N. associated International Telecommunication Union (ITU) coordinates world-wide agreements and harmonisation of telecommication systems.

IEEE 802.11 Radio Frequencies

- 2.4GHz
  - The Industrial, Scientific and Medical (ISM) band is a section of the radio frequency spectrum that is unlicensed – users do not have to seek FCC, ODTR… approval to operate short range devices in this piece of the spectrum.
  - The band extends from 2.4GHz to 2.5GHz and has an associated maximum permitted radiated power (EIRP) of 100mW according to European regulations.
  - No reliability is guaranteed in this band, WLANs do not receive regulatory protection.
  - Microwave ovens operate at 2.45GHz.

IEEE 802.11 Radio Frequencies

- 5GHz
  - The US FCC released 3 bands in the 5GHz range for short range devices, calling them the Unlicensed National Information Infrastructure (UNII) bands. The CEPT/ECC has other ideas:
    - FCC UNII
      - 5.15 - 5.25GHz indoor use 50mW EIRP
      - 5.25 - 5.35GHz indoor/ outdoor use 250mW EIRP
      - 5.725 - 5.825GHz point-to-point bridging 1W EIRP
    - CEPT
      - 5.15 – 5.35GHz HIPERLAN indoor use 200mW EIRP
      - 5.47 – 5.725GHz HIPERLAN indoor/outdoor use 1W EIRP
      - 5.725 – 5.875GHz ISM 25mW EIRP (under review)
  - The CEPT/ECC requires devices to use dynamic frequency allocation and transmitter power control in their first two bands.
  - According to the COMREG, there are plans to allocate the 17GHz and 60GHz bands for similar WLAN applications.

802.11

- **'802.11'**
  - In 1997 the 802.11 MAC and PHY WGs defined specifications for 3 physical layers (PHY) and a medium-access control layer (MAC).
  - 802.11 PHY:
    - IR – not widely deployed
    - 2 spread spectrum radio layers at **2.4GHz**
      - FHSS - Frequency Hopping Spread Spectrum
      - DSSS - Direct Sequence Spread Spectrum
  - The transmission speed was limited to 1-2Mbps
  - 802.11 PHY is commonly referred to as just '802.11'
- The IEEE continued to investigate faster radio layers, developing two new PHY standards, 802.11**a** and 802.11**b**

IEEE 802.11 Common Standards

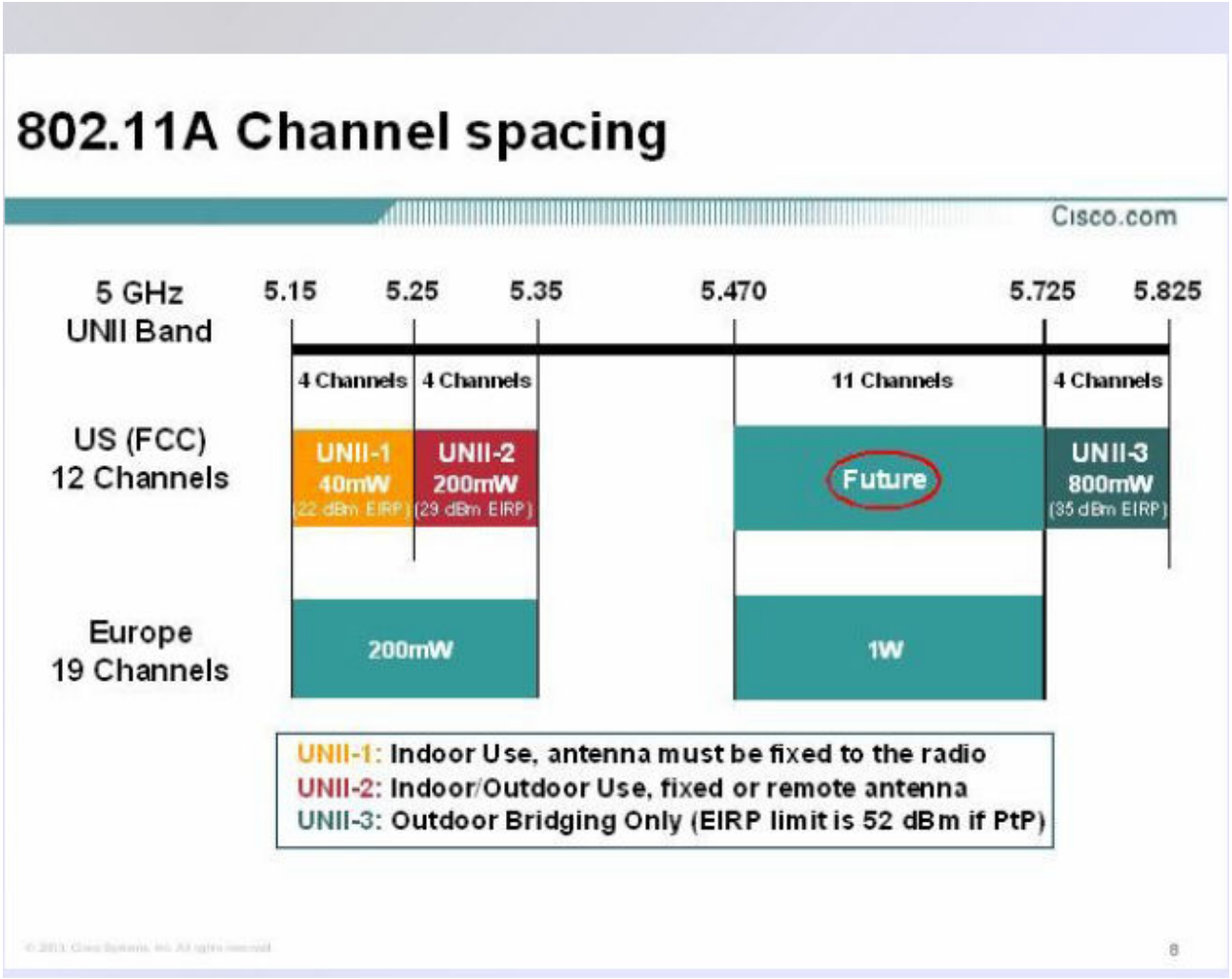
- 802.11b data-rates (modulation schemes):
  - 1Mbps (BPSK), 2Mbps (QPSK), 5.5Mbps (CCK), 11Mbps (CCK)
- 802.11a and 802.11g data-rates:
  - 6, 9, 12, 18, 24, 36, 48, 54 Mbps
  - OFDM + BPSK/QPSK/16QAM/64QAM
  - 802.11g also supports 802.11b data-rates and modulations (backwards compatible)

802.11

- **802.11a**
  - Physical layer uses Orthogonal Frequency Division Multiplexing (OFDM) in the **5GHz** band.
  - Provides a theoretical bandwidth of 54Mbps in throughput steps of 6, 9, 12, 18, 24, 36, 48 and 54 Mbps
  - Updated standard finished in 1999, but only certified for use in US as it conflicts with European regulations
  - Similar to ETSI standard HIPERLAN II

802.11a channels

- Each channel is 20MHz wide

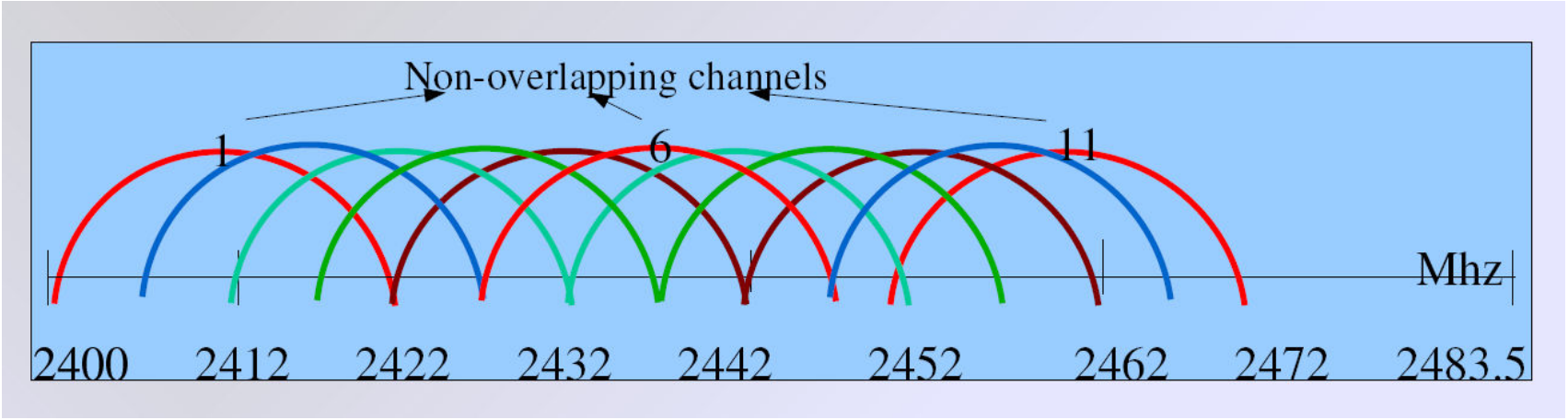


802.11

- **802.11b**
  - Released in 1997
  - Most commonly deployed version of the 802.11 family
  - Promises operational speeds of 5.5Mbps and up to 11 Mbps at **2.4 GHz**
  - The physical layer applies Complementary Code Keying (CKK) and Packet Binary Convolutional Coding (PBCC) modulation techniques to DSSS signals.

802.11b channels

- Each channel is 22MHz wide
- Adjacent channels overlap
- Non-overlapping channels: 1, 6, 11



802.11

- **802.11g**
  - Speeds of up to 54Mbps
  - Physical layer uses OFDM, as does 802.11a, but at 2.4GHz
  - As its at 2.4GHz it must be interoperable with the 802.11 PHY standard. 802.11 PHY does not 'understand' OFDM
  - Delayed approval as industry heavyweights Texas Instruments and Intersil wanted their own modulation schemes used at the physical layer in addition to OFDM
    - TI – Complementary Code Keying/OFDM
    - Intersil - PBCC

802.11

- **802.11h**
  - Essentially 802.11a with spectrum management functionality, namely:
    - Dynamic channel allocation
    - Transmit power control
  - Required for pan-European regulatory approval as it allows the technology to co-exist in the 5GHz band with other users
  - Select channels based on real-time feedback
  - Adjust transmit power to environmental needs – indoor/outdoor use, network density etc.

IEEE 802.11 Spread Spectrum

- Traditional radio communications focussed on the use of narrow band signals – FM radio etc.
- Spread spectrum works by taking a narrow band signal and using mathematical techniques to diffuse the signal power over a larger range of frequencies.
- Both the transmitter and receiver agree on the same technique, allowing the receiver to reconstitute the narrow band signal from the diffused signal.
- Looks like noise to narrow-band receivers
- Co-patented by Austrian-born actress Hedy Lamarr

in 1942. Billed by Hollywood's Louis B. Mayer as the as the 'most beautiful woman in the world', the model for Catwoman in the original Batman comics and the first actress to appear nude on film in a German film, 'Extasy', in 1932.

Types of Spread Spectrum

- Frequency hopping – **FHSS**
  - Systems jump form one frequency to another in a pseudo-random pattern, transmitting a short burst of information in each subchannel.
- Direct Sequence –**DSSS**
  - The power is spread out over a wider frequency band using mathematical functions.
- Orthogonal Frequency Division Multiplexing –**OFDM**
  - The available channel is divided into several subchannels and portions of the signal are encoded across each subchannel in parallel. A similar technique, Discrete Multi-Tone (DMT) technique, is used by some DSL modems.

802.11 MAC

- The same Medium Access Control (MAC) layer is used for all variants of the 802.11 physical layer.
- Why is there a need for a MAC? What are the problems?
  - Multiple devices want to access the same medium – 'ether'
  - Unlicensed devices must assume that interference exists and work around it.
  - Transmission costs energy –device lifetime, MAC must be efficient
  - Devices have different service requirements:
    - Real-time – voice, video
    - Best-effort, buffered – data
  - Hidden terminal, exposed node problems
  - The schemes may be centralised or distributed

802.11 MAC

- The MAC protocol must define a set of rules for the orderly sharing of a scarce medium – the wireless channel – by multiple mobile nodes, while solving the problems and supporting the services mentioned above.

- 802.11 MAC does not differ radically from other IEEE 802 standards.
  - Its an adaptation of Ethernet-style networking to radio links.
  - Ethernet uses a Carrier Sense Multiple Access with Collision Detection (**CSMA/CD**) scheme to control access to the transmission medium.
  - Collisions waste valuable transmission capacity so 802.11 uses Collision Avoidance (**CSMA/CA**) – may also be half-duplex
  - 802.11 uses a distributed access scheme
  - 802.11 incorporates positive acknowledgements of data transfer

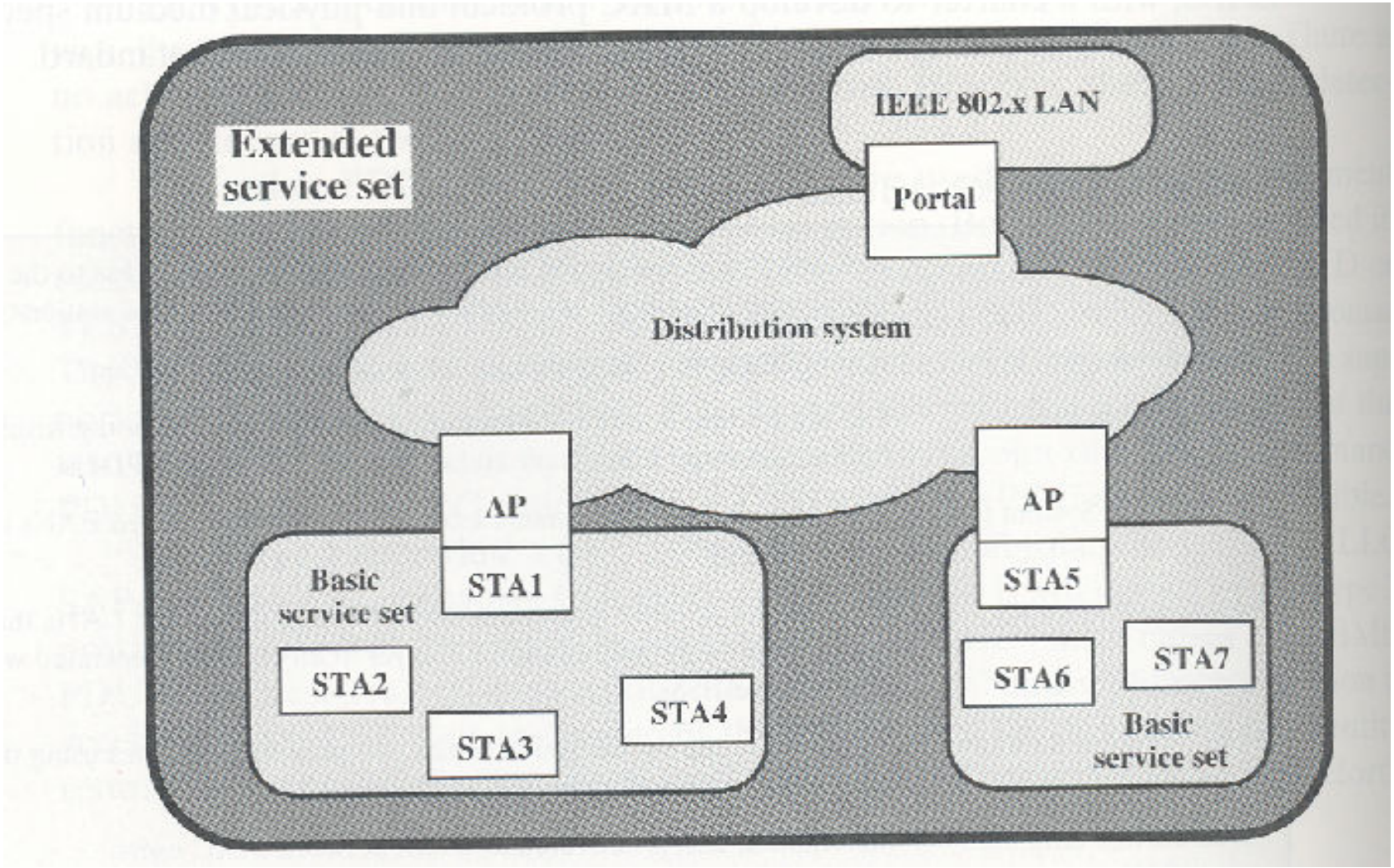
802.11 MAC

- For larger frames of data, beyond a specified threshold, 802.11 allows the use of Request To Send (**RTS**) and Clear To Send (**CTS**) signals to clear an area for a given time for data transfer
  - An RTS frame is sent and it silences nodes that hear it.
  - If the target station hears the RTS it responds with a CTS which also silences nodes for a specified period.
  - The data frame is sent and then positively acknowledged
- 802.11 MAC provides 2 modes for access and timing
  - Distributed Coordination Function (**DCF**) – CSMA/CA: check to see if the radio channel is clear before sending, wait for an Inter Frame Space (**IFS**) period, send data. To avoid collisions, stations use a random backoff after each frame, with the first transmitter seizing the channel. DCF may use the RTS/CTS function in some situations.
  - Point Coordination Function (**PCF**) – Contention-free services, only provided in infrastructure networks. Special stations, called access points, control the sending of data frames by polling mobile stations in turn and allowing them to send data at a faster rate than in DCF. PCF is an optional function.

802.11 Networks

- 802.11 network components:
  - **Access points**: Frames on an 802.11 network must be converted into other types of frames for delivery to hosts/servers on other networks. Access points perform a wireless-to-wired bridging function.
  - **Stations**: Computing device with wireless network interfaces.
  - **Distribution system**: When several access points are connected to cover a large area, they must communicate to track the movement of mobile stations. 802.11 does not specify a distribution system, but in most commercially successful products, Ethernet is used as the backbone network technology.
  - **Wireless medium**: 802.11 uses the wireless medium to move frames from station to station. Multiple physical layers, as discussed, have been developed to support the 802.11 MAC

802.11 Networks



802.11 Networks

- The main building block of an 802.11 network is called a Basic Service Set (**BSS**).
  - A group of stations that communicate with each other.
  - Communication takes place within a Basic Service Area, an area defined by the propagation characteristics of the wireless medium.
  - There are two types of BSS
    - **Independent BSS**: Stations communicate directly with other stations in direct communication range, generally short-lived arrangements supporting a small number of stations.
    - **Infrastructure BSS:** An access point is used for all communication between nodes, including nodes in the same basic service area. Used for longer-lived networks, allows for network management. Stations must associate with an access point – like plugging into the network on Ethernet. Mobile stations initiate the process and access points may grant/deny access.
    - **Extended BSS:** A number of BSSs connected by a backbone.

802.11

- 802.11 provides weak security: WEP shared key and open system authentication. 802.11i is looking at new standards.
- WECA – The Wireless Ethernet Compatibility Alliance provides a certification program
  - Allows vendors to have their products independently tested for interoperability
  - Certified products may then carry the **Wi-Fi** mark, 802.11a will use the **Wi-Fi5** mark
- Manufacturers
  - Texas Instruments
  - Intersil
  - Atheros
  - Agere (formerly Lucent)
  - Intel (embedded in mobile processor chips)