ECE 442/510

Internet of Things and Cyber Physical Systems

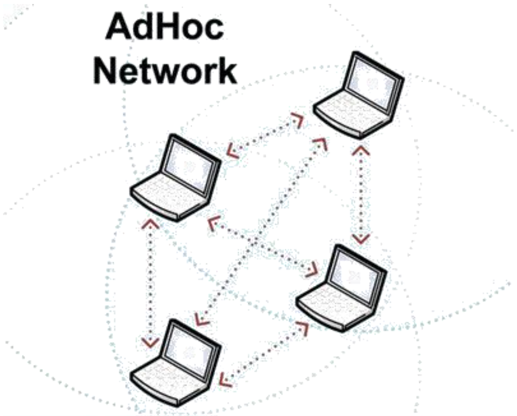
Lecture 7: Wireless Technologies and IoT

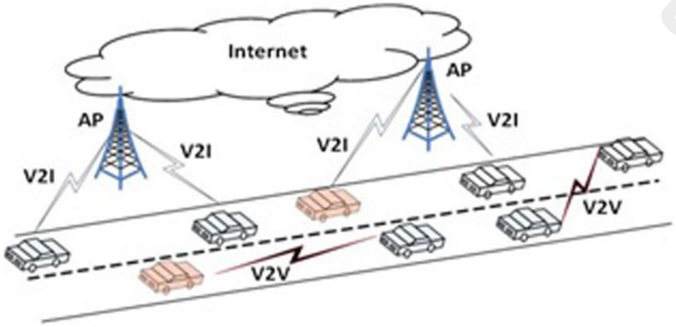
Summer 2022

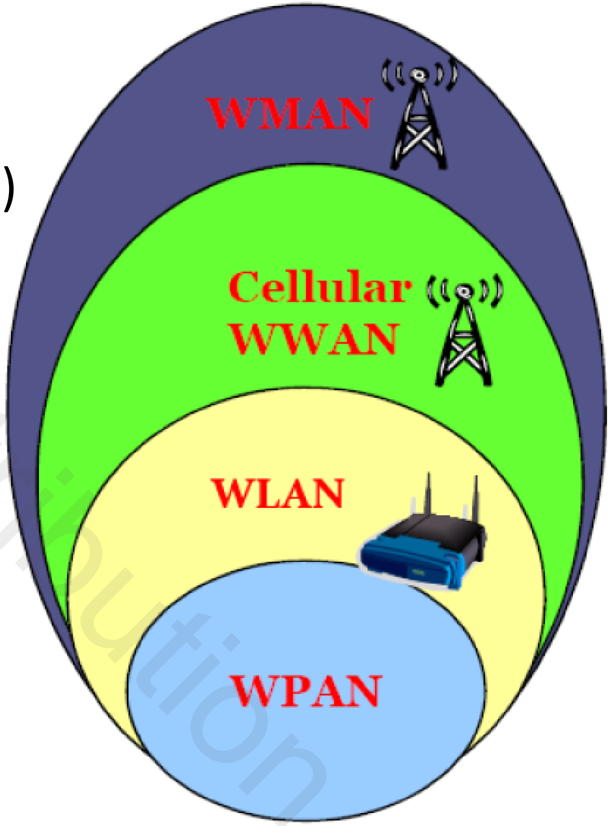
Jafar Saniie & Won-Jae Yi

Existing Wireless Networks

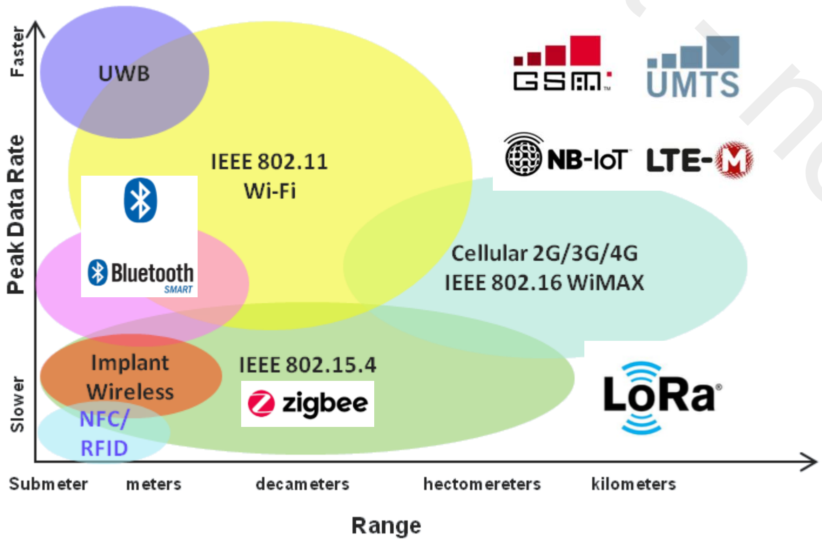
- Wireless Metropolitan Area Network (WMAN)
- Cellular/Wireless Wide Area Network (WWAN) (GSM, WCDMA, EV-DO)
- Wireless Local Area Network (WLAN)
- Wireless Personal Area Network (WPAN)
- Ad hoc Networks
- Sensor Networks
- Emerging Networks (variations of ad hoc networks)
  - Info-stations
  - Vehicular Networks



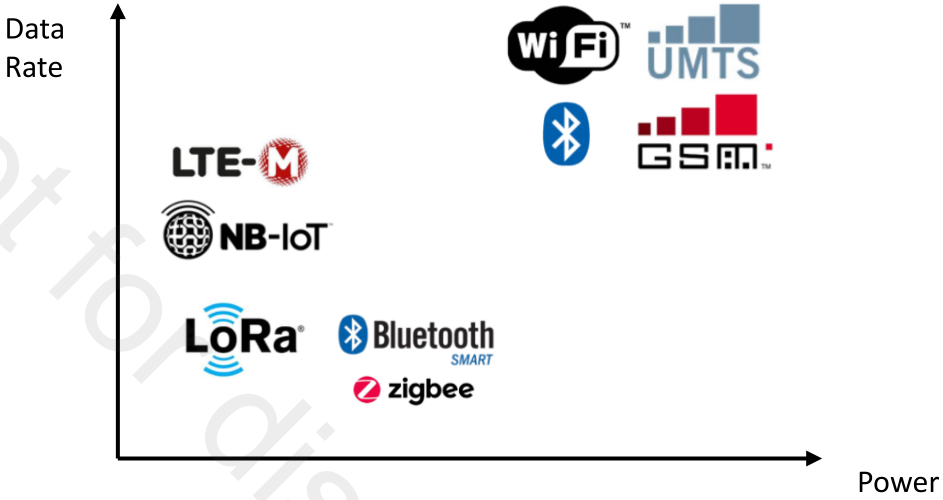




Data Rate vs. Range

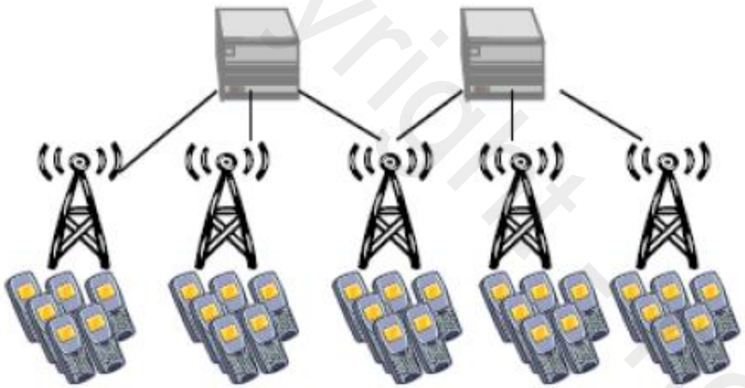


Data Rate vs. Power



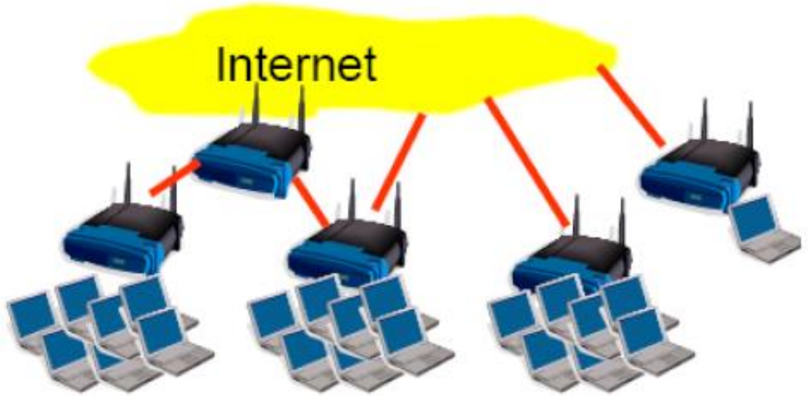
- NB-IoT and LTE-M are protocols/services for IoT devices from wireless carriers
- Long Range (LoRa) can be useful for agricultural automation (smart farming)
- Bluetooth, ZigBee, Wi-Fi operates 2.4 GHz range

Network Architectures



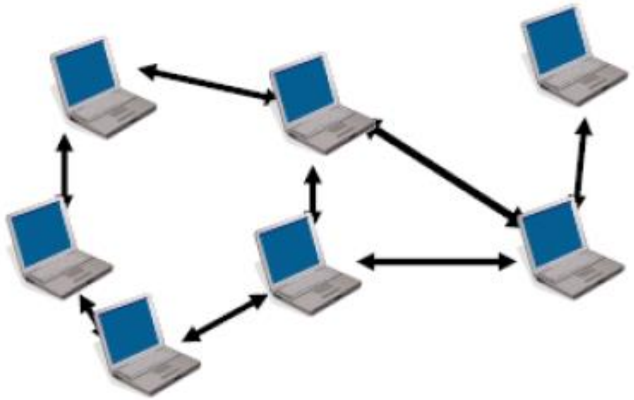
Cellular Networks (hierarchical systems)

☺ QoS + mobility ☹ $$$, lack of innovations



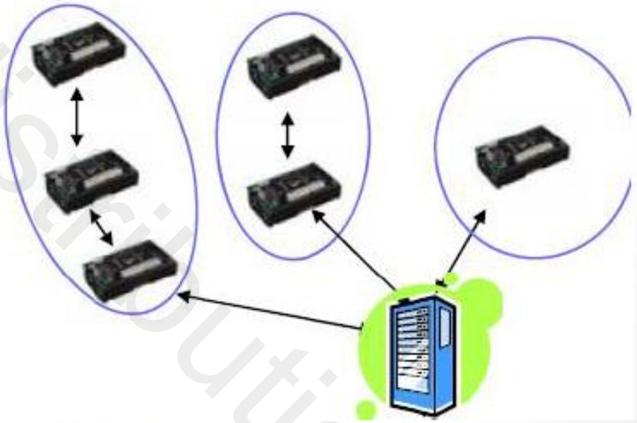
WLAN / Mesh networks

☺ Simple, cheap ☹ Poor management



Ad hoc networks

☺ no infrastructure cost ☹ no guarantee



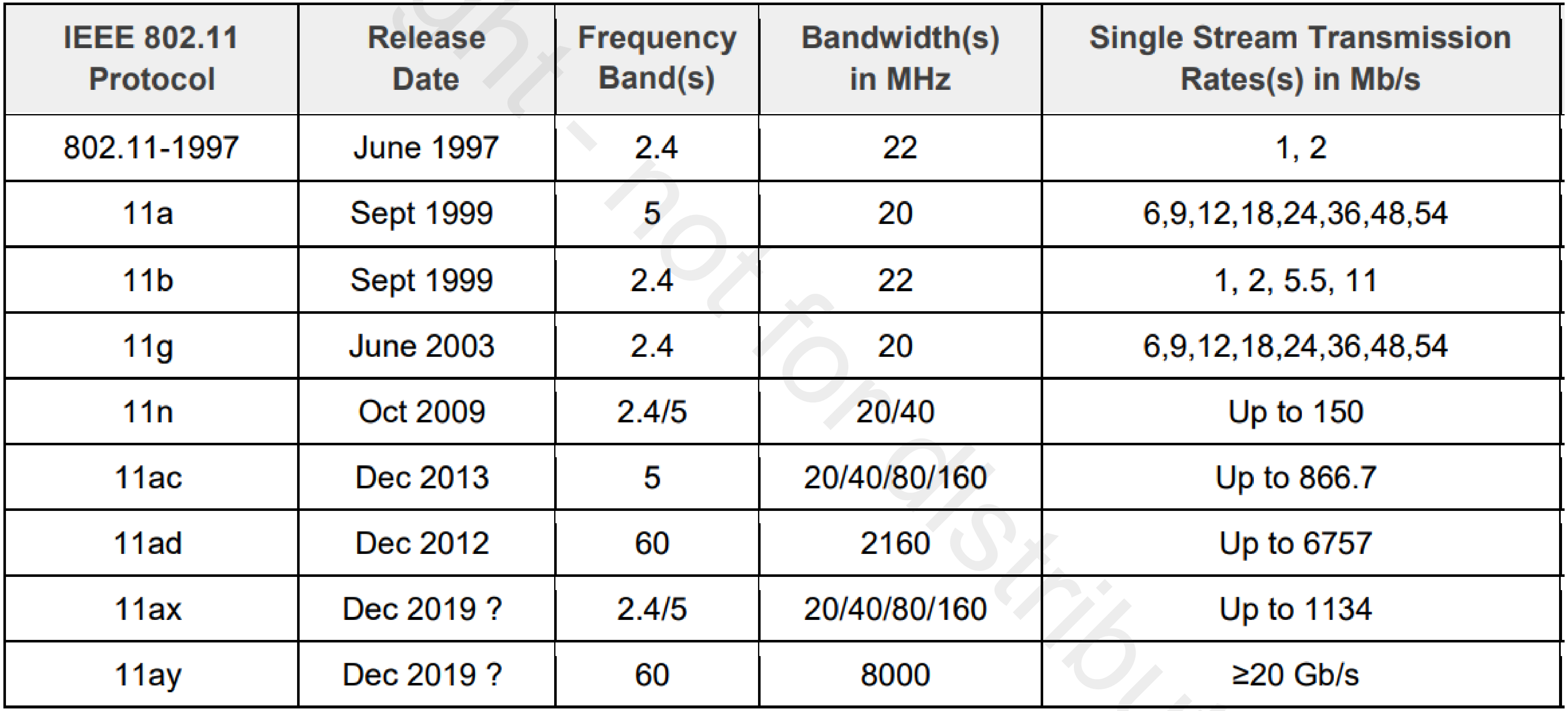
Sensor networks

☹ Energy limited, low processing power

IEEE 802.11 – Wi-Fi

- A trademark of the Wi-Fi Alliance
- The brand name for products using the IEEE 802.11 family of standards
- Commonly used for wireless local area network (WLAN)
- Point-to-Multipoint (Access Point)
- Point-to-Point (Ad hoc)
- Multipoint-to-Multipoint (Mesh Network)

IEEE 802.11 Protocols

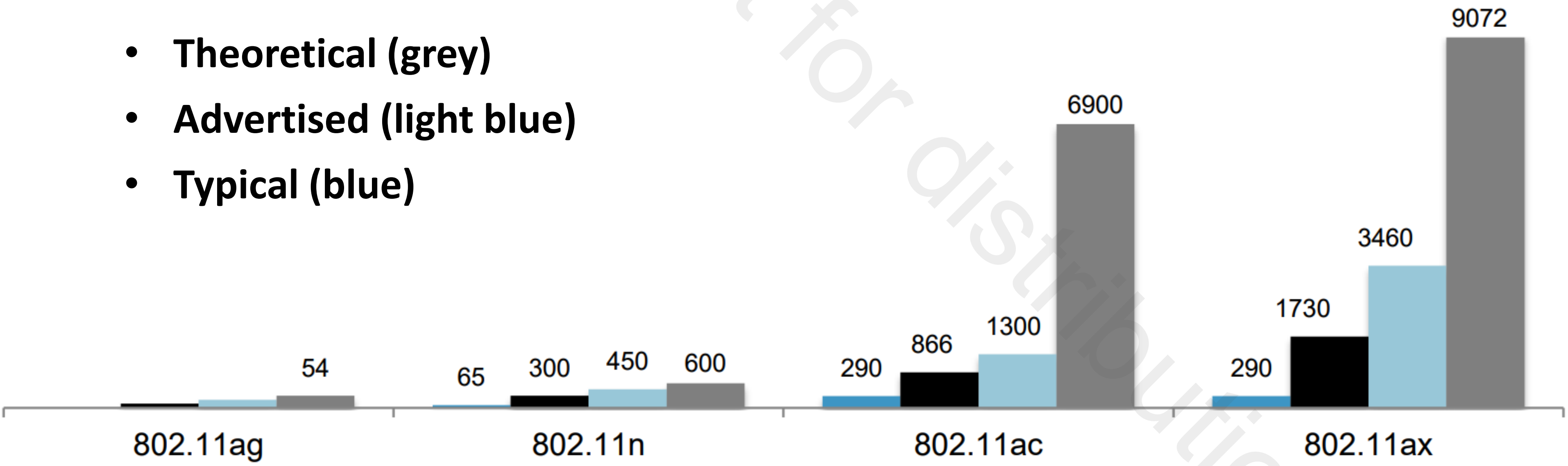


IEEE 802.11 Protocol	Release Date	Frequency Band(s)	Bandwidth(s) in MHz	Single Stream Transmission Rates(s) in Mb/s
802.11-1997	June 1997	2.4	22	1, 2
11a	Sept 1999	5	20	6,9,12,18,24,36,48,54
11b	Sept 1999	2.4	22	1, 2, 5.5, 11
11g	June 2003	2.4	20	6,9,12,18,24,36,48,54
11n	Oct 2009	2.4/5	20/40	Up to 150
11ac	Dec 2013	5	20/40/80/160	Up to 866.7
11ad	Dec 2012	60	2160	Up to 6757
11ax	Dec 2019 ?	2.4/5	20/40/80/160	Up to 1134
11ay	Dec 2019 ?	60	8000	≥20 Gb/s

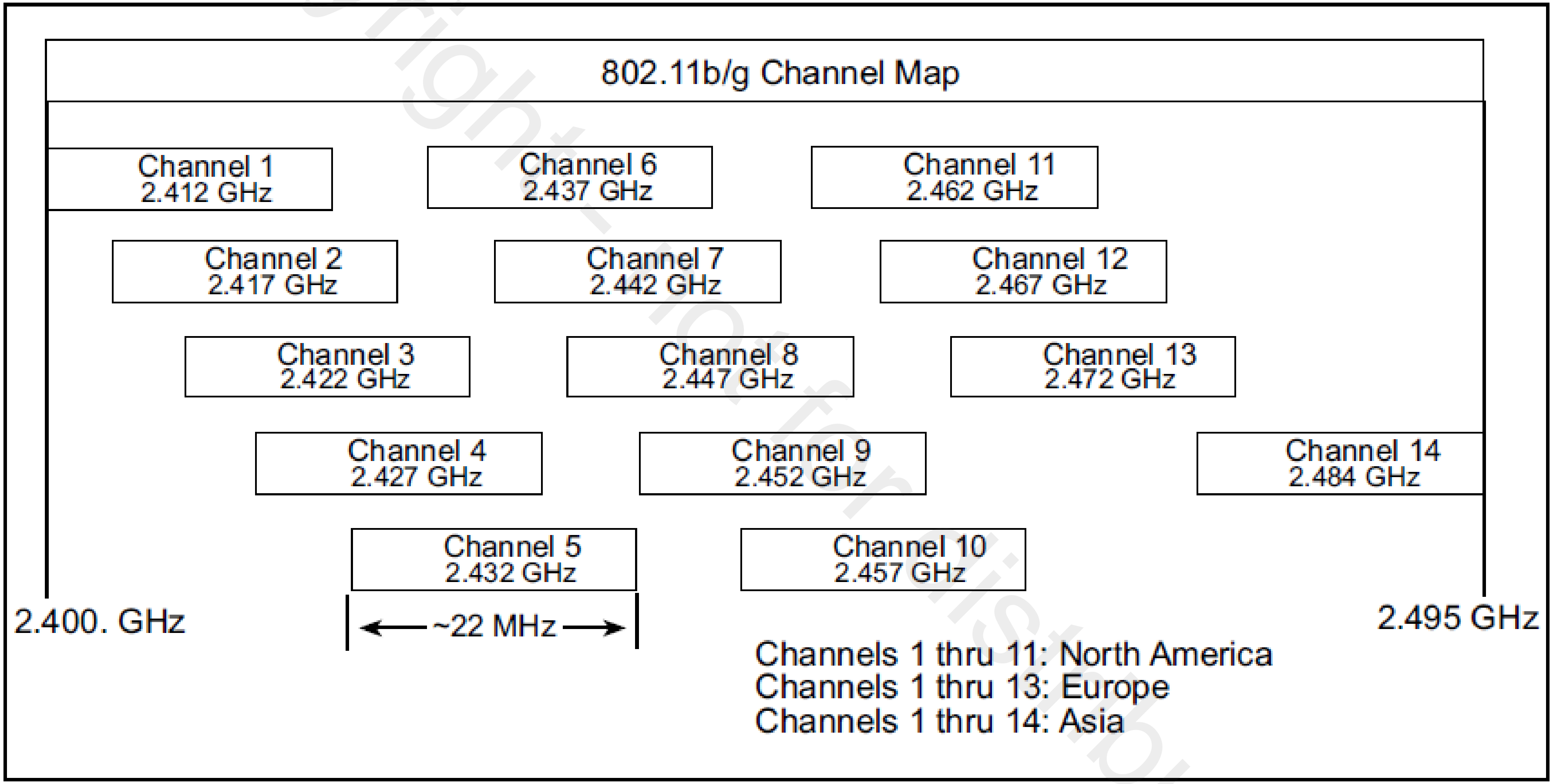
Wi-Fi Data Rates

- In practice, typical rates depend on many factors
  - signal degradation with distance
  - modulation rate and forward error correction coding
  - bandwidth, MIMO multiplier, guard interval and typical error rates
  - back-off/rate adaptation parameters

- **Theoretical (grey)**
- **Advertised (light blue)**
- **Typical (blue)**



Wi-Fi Channels (2.4GHz)



802.11b/g Channel Map

Channel 1
2.412 GHz

Channel 6
2.437 GHz

Channel 11
2.462 GHz

Channel 2
2.417 GHz

Channel 7
2.442 GHz

Channel 12
2.467 GHz

Channel 3
2.422 GHz

Channel 8
2.447 GHz

Channel 13
2.472 GHz

Channel 4
2.427 GHz

Channel 9
2.452 GHz

Channel 14
2.484 GHz

Channel 5
2.432 GHz

Channel 10
2.457 GHz

2.400. GHz

~22 MHz

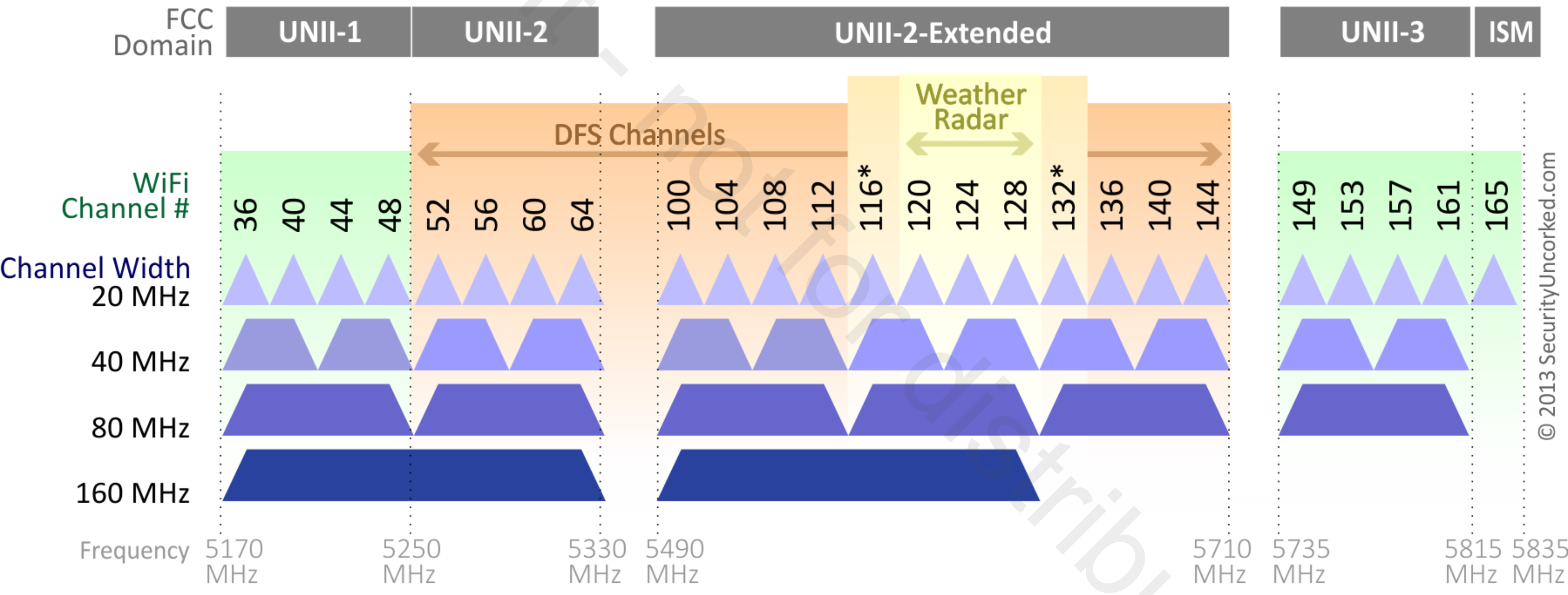
2.495 GHz

Channels 1 thru 11: North America
Channels 1 thru 13: Europe
Channels 1 thru 14: Asia

- **Guard Band (2 MHz)** to reduce signal interference between Channels

Wi-Fi Channels (5GHz)

802.11ac Channel Allocation (N America)



*Channels 116 and 132 are Doppler Radar channels that may be used in some cases.

- DFS (Dynamic Frequency Selection) channels are reserved for radar (e.g., military radar, satellite communication, weather radar)

Wi-Fi Direct

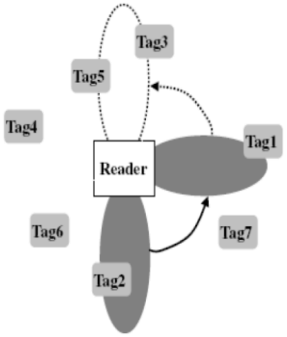
- Connects devices directly, with or without a Wi-Fi network or hotspot available
- Makes the connection to open a world of applications, including content sharing, synchronizing data, printing, gaming and more
- Connects with almost any Wi-Fi CERTIFIED device
- Designed for portable and stationary devices
- Wireless displays (Intel’s WiDi, Miracast)
- “Pairing” of Wi-Fi Direct devices can be setup by using Near Field Communication (NFC), Bluetooth, a button press, manual…

Challenges in Wi-Fi

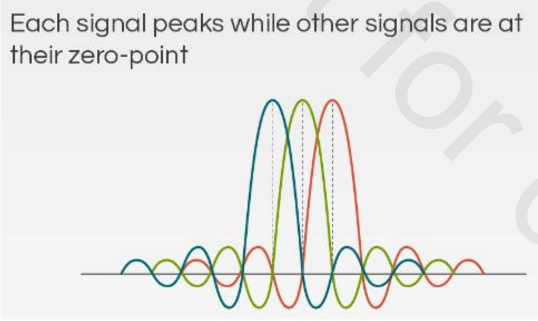
- Explosion of users, devices…
- Interference, interference, interference…
  - Heavy interference/contention when accessing the AP and there may be no QoS support (some do now..)
  - Inter-AP interference
  - Interference from other devices (microwaves, cordless phones, wireless keyboard/mouse) in the same frequency band (2.4 GHz)
- Mobility Support
  - Seamless roaming when users move between APs within same SSID (Service Set Identifier)
  - Normally low speed around 3 – 10 mph

Anti-Collision Protocols for Communications

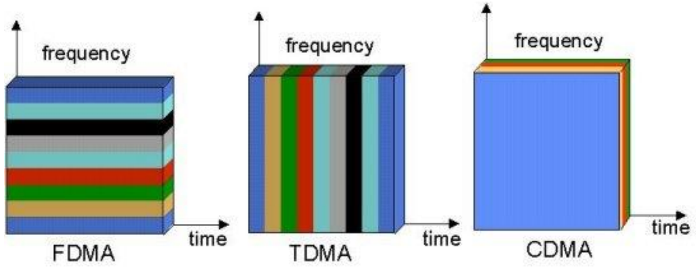
- SDMA : Space Division Multiple Access
- FDMA : Frequency Division Multiple Access
- TDMA : Time Division Multiple Access
- CDMA : Code Division Multiple Access
- OFDMA : Orthogonal FDMA
- NOMA : Non-Orthogonal Multiple Access (distinguished by power levels)

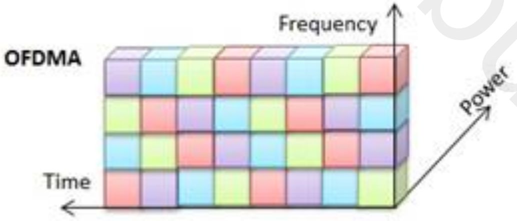


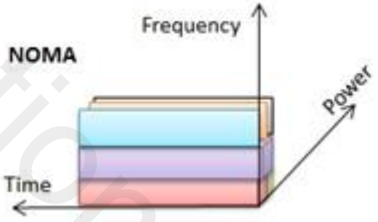
SDMA



OFDM: Orthogonal Frequency Division Multiplexing







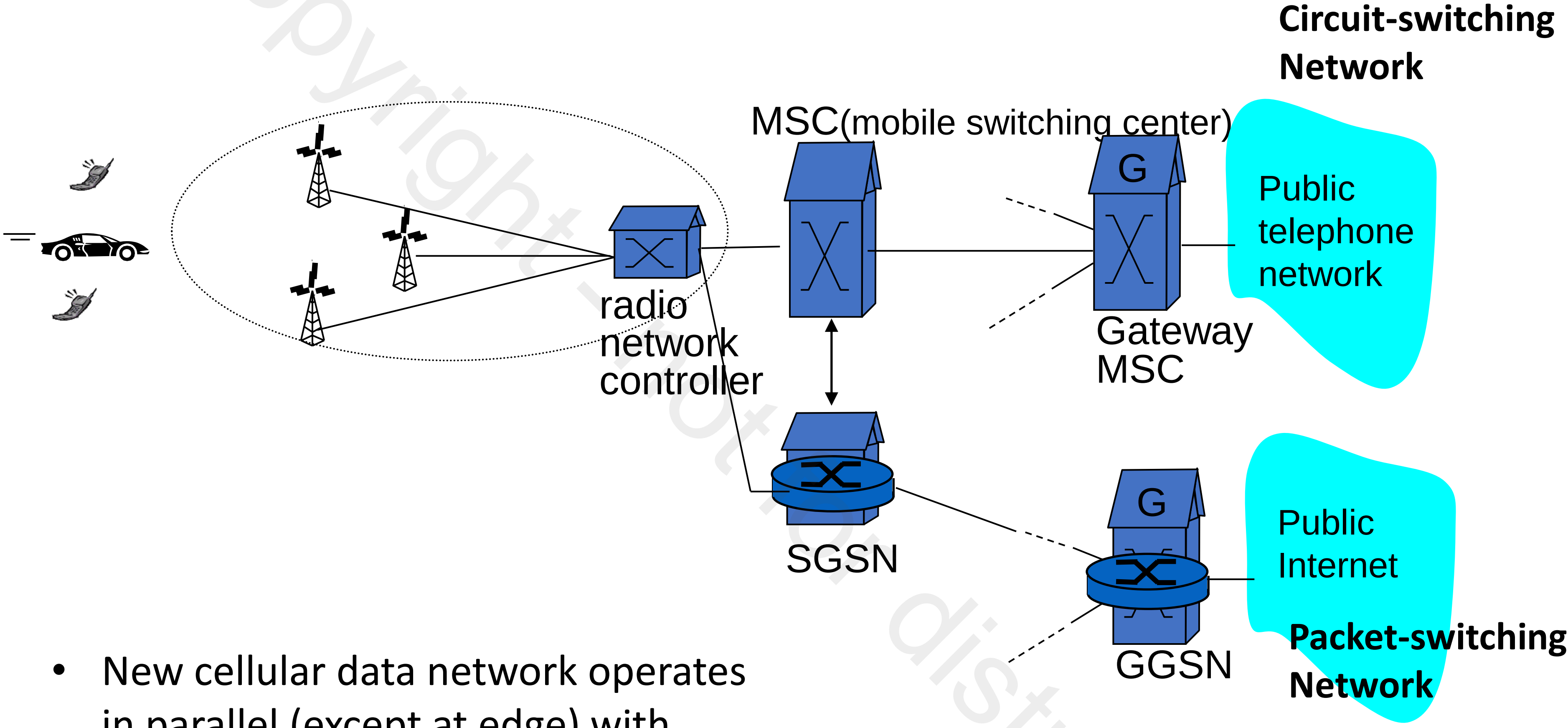
1G Mobile Network

- Wireless telephone and mobile communication technology based on FDMA
- Digital signaling to communicate with towers, the phone signals after establishing the connection is analog
- The first commercially automated cellular network (1G generation) was launched in Japan by NTT (Nippon Telegraph and Telephone) in 1979
- In 1981, this was followed by the simultaneous launch of the Nordic Mobile Telephone (NMT) system in Denmark, Finland, Norway and Sweden. NMT was the first mobile phone network featuring international roaming
- The first 1G network launched in the USA was Chicago-based Ameritech in 1983 using the Motorola DynaTAC mobile phone

2G Mobile Network

- Commercially launched on the GSM standard in Finland (1991)
  - Conversation digitally encrypted
  - Significantly more efficient in spectrum use
  - Mobile data service (SMS, text message)
  - 2G network can be divided into two categories: TDMA and CDMA
  - TDMA: Time Division Multiple Access
  - CDMA: Code Division Multiple Access
- GSM: Global Systems for Mobile communication (TDMA based)
  - Digital, circuit switched network system supporting both voice and digital data (900 MHz or 1800MHz)

3G Mobile Network



- New cellular data network operates in parallel (except at edge) with existing cellular voice network
- Voice network unchanged in core
- Data network operates in parallel

Serving GPRS Support Node (SGSN)

Gateway GPRS Support Node (GGSN)

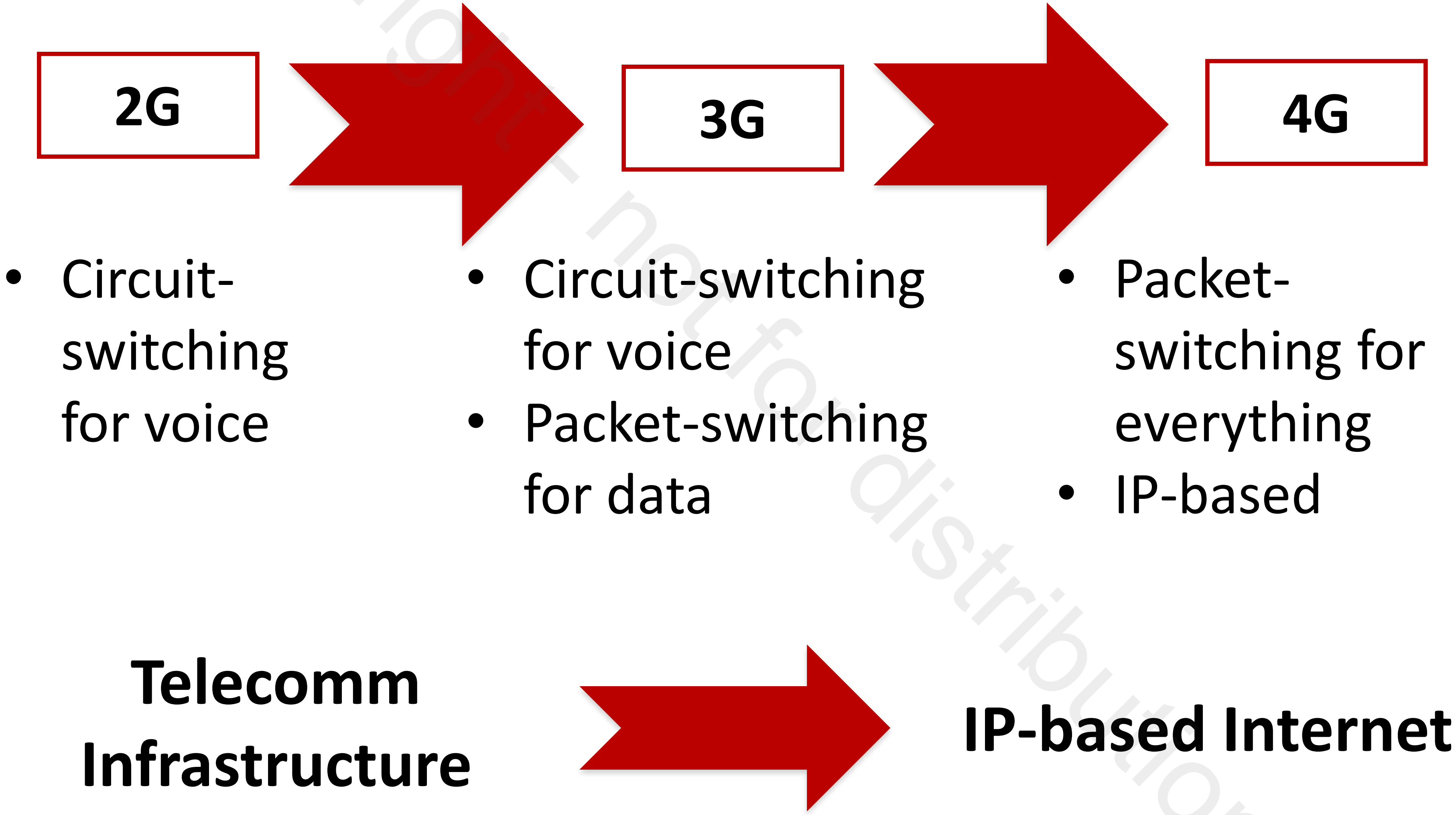
4G Mobile Network

- 4G network
  - 4th generation mobile communication technology that provides high speed access to phone and data service
- Two competing standards
  - 4G LTE (Long Term Evolution)
  - ~~WiMAX (IEEE 802.16)~~
- 4G LTE is the first global standard
  - Increased speed
  - IP-based network → Packet-switching Network (voice and data)
  - New air interface: OFDMA (Orthogonal Frequency Division Multiple Access), MIMO (Multiple Input Multiple Output, Multiple antennas)
  - New service paradigm (e.g., VoLTE, Wi-Fi Callings)

4G LTE General

- 4G LTE is a mobile communications standard that provides access for mobile devices to core network
- It is an evolution of the GSM/UMTS standards (from phones to Internet)
- The goal of LTE was to increase the capacity and speed of wireless data networks using new DSP techniques and modulations that were developed around the turn of the millennium.
- A further goal was to redesign and simplification of the network architecture to an IP-based system
- The LTE wireless interface is incompatible with 2G and 3G networks

Network Architecture Evolution



2G

- Circuit-switching for voice

3G

- Circuit-switching for voice
- Packet-switching for data

4G

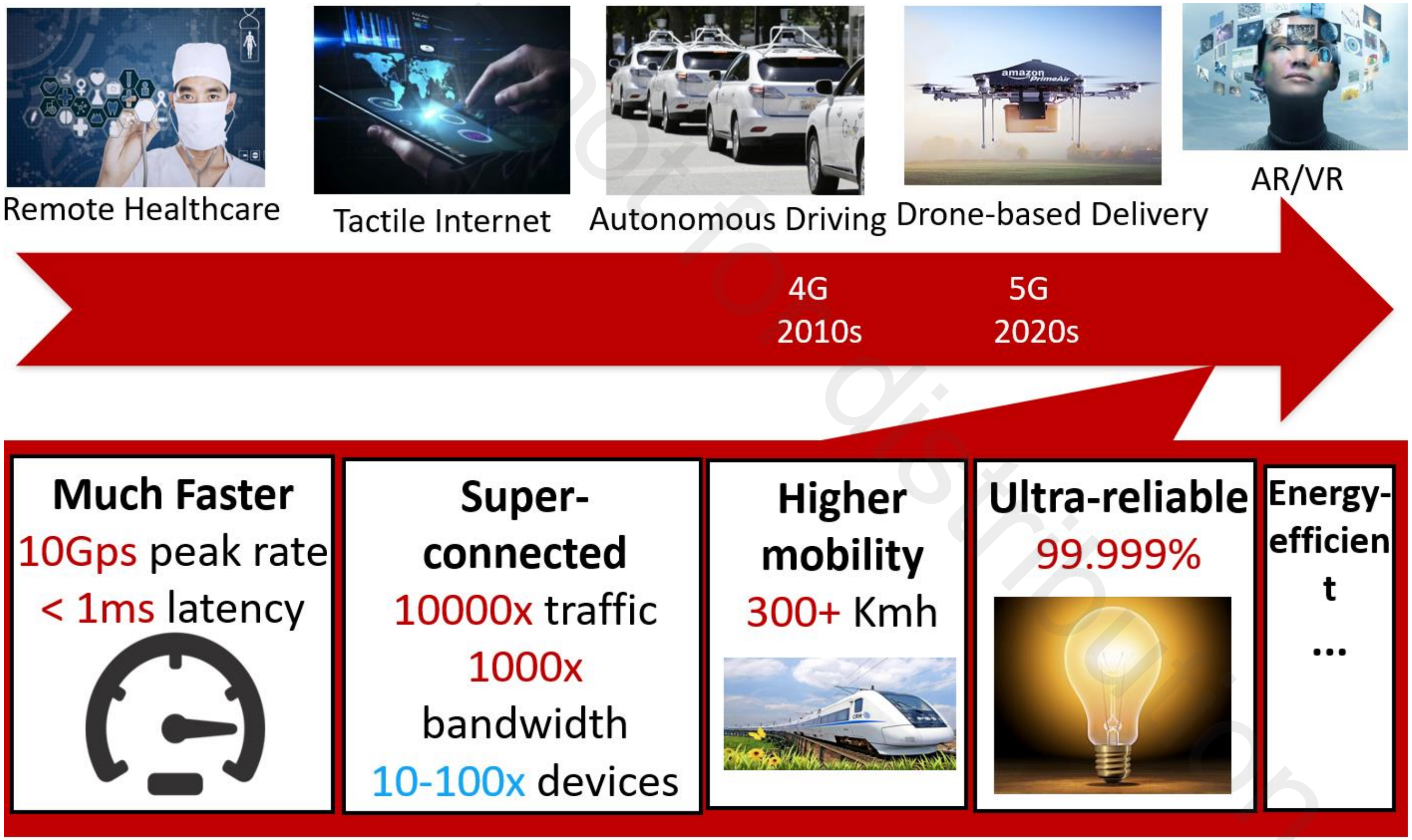
- Packet-switching for everything
- IP-based

Telecomm Infrastructure

IP-based Internet

5G (5th Generation)

- NOMA (Non-Orthogonal Multiple Access)
  - Multiple users utilize same frequency band, but with different power levels to be distinguished



Remote Healthcare

Tactile Internet

Autonomous Driving

Drone-based Delivery

AR/VR

4G
2010s

5G
2020s

Much Faster
10Gps peak rate
< 1ms latency

Super-connected
10000x traffic
1000x bandwidth
10-100x devices

Higher mobility
300+ Kmh

Ultra-reliable
99.999%

Energy-efficient
...

Bluetooth

- Wireless Personal Area Networks (WPAN)
- Design goals
  - Cable replacement
  - Low cost, low power
  - Small size, ad-hoc networks
  - For mobile devices and communication including voice and data
- Standard: IEEE 802.15.1 → Bluetooth SIG (Special Interest Group)
- 1994, Ericsson gets interested in wireless connections from mobile telephones to other devices like PDAs (Personal Digital Assistant) and accessories like Headsets
- Forming the SIG (Special Interest Group) with 4 other members (IBM, Intel, Nokia, Toshiba) in order to develop a wireless standard for communication between mobile devices

Bluetooth Versions

Version	Data rate	Feature
1.2	721 kb/s	
2.0 + EDR	3 Mb/s	Enhanced Data Rate (EDR)
3.0 + HS	24 Mb/s	High-Speed
4.0	1 Mb/s (BLE)	Bluetooth Low Energy (BLE)
5	2 Mb/s	

Bluetooth Connection Types

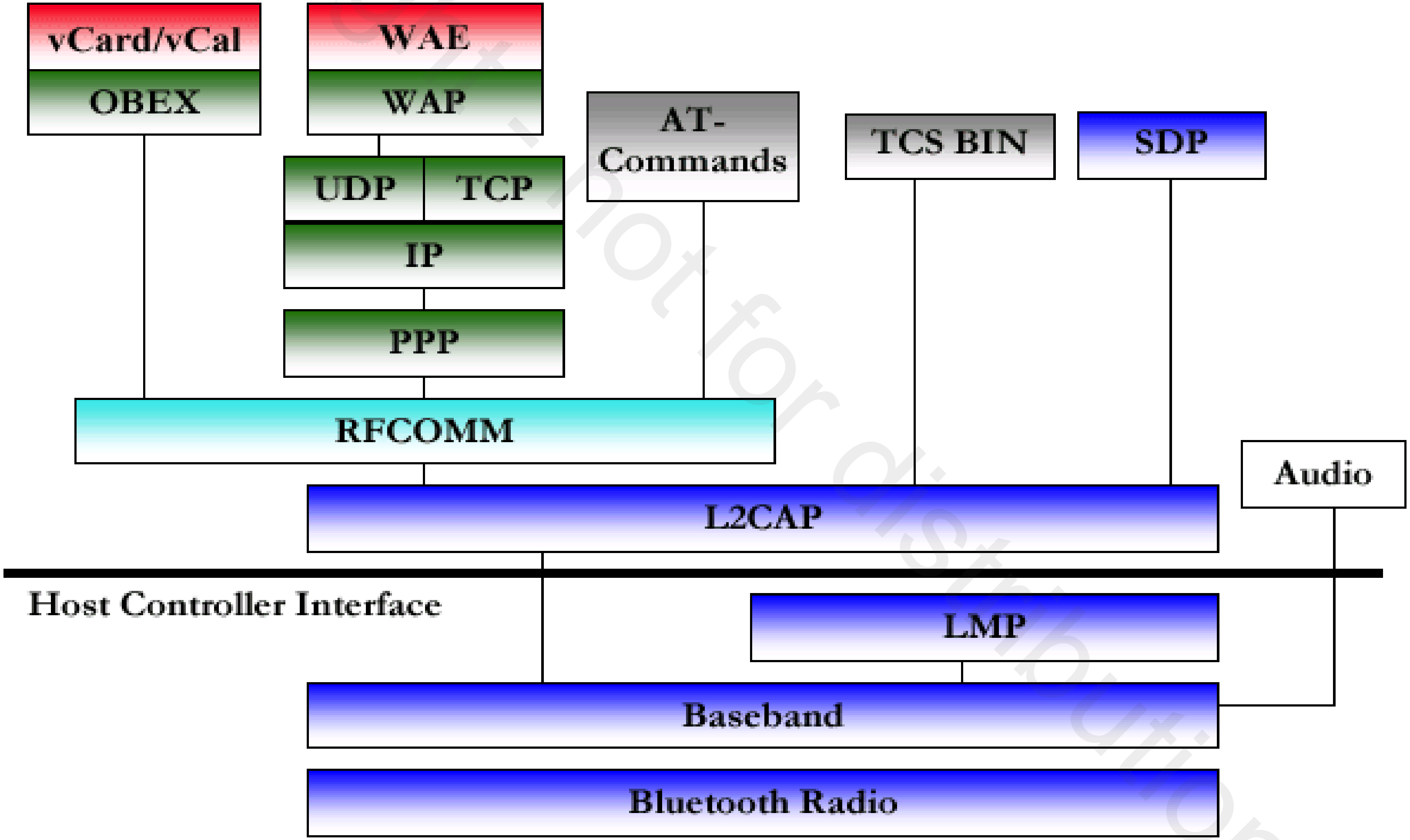
- **Classic**: 1 to 1 (serial communication, audio connection)
- **Bluetooth Low Energy (BLE)**: 1 to Many (publish-subscribe)

Bluetooth vs. Wi-Fi

	Bluetooth	Wi-Fi
Specifications authority	Bluetooth SIG	IEEE, WECA
Year of development	1994	1991
Bandwidth	Low (typically 800 Kbps)	High (11 Mbps+)
Hardware requirement	Bluetooth adapter on all the devices connecting with each other	Wireless adapters on all the devices of the network, a wireless router and/or wireless access points
Cost	Low	High
Power Consumption	Low	High
Frequency	2.4 GHz	2.4 GHz/5GHz
Security	It is less secure	It is more secure
Range	short	long
Primary Devices	Mobile phones, mouse, keyboards,office and industrial automation devices	Notebook computers, desktop computers, servers
Ease of Use	Fairly simple to use. Can be used to connect up to seven devices at a time. It is easy to switch between devices or find and connect to any device.	It is more complex and requires configuration of hardware and software.

Bluetooth

- **Bluetooth Protocol Stack**



Bluetooth – Layers

- **Bluetooth Radio**
  - Operates in the 2.4 GHz ISM (industrial, scientific, medical) Band
  - Accomplishes spectrum spreading by frequency hopping (FHSS) from 2.402 GHz to 2.480 GHz
  - 4 different power classes (not version)
    - Class 1: long range (100m, 100mW)
    - Class 2: mid range (10m, 1 – 2.5mW)
    - Class 3: short range (0.1 – 10m, 1mW)
    - Class 4: shorter range (<0.5m, 0.5mW)

Bluetooth – Layers

- **Baseband**
  - Physical layer of the Bluetooth
  - Error correction, flow control, hopping sequence, security
  - Hopping through 79 channels (1 MHz per channel)
  - Data is divided in packets
    - Access code: e.g., timing synchronization
    - Header: e.g., packet numbering, flow control, slave address
    - Payload: voice, data or both
  - Security modes
    - Non-secure
    - Encryption enforced by application layer or link layer
    - Trusted/untrusted device
    - Services
      - Require authorization and/or authentication
      - open to all devices

Bluetooth – Layers

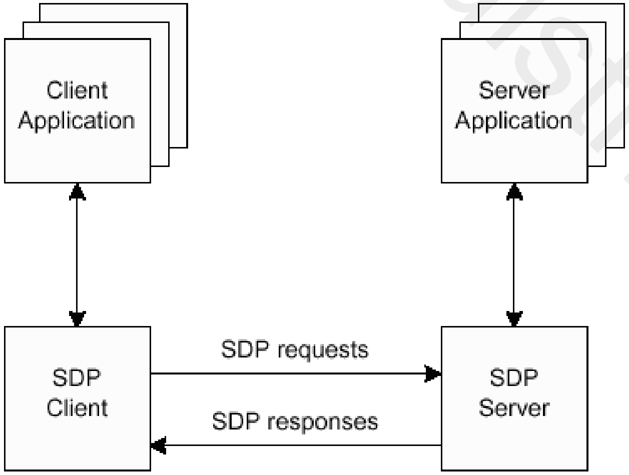
- **LMP (Link Manager Protocol)**
  - Provides authentication, link setup and link configuration including power surveillance
  - Takes place as a service provider
  - Communication with LM PDUs (protocol data units)
- **HCI (Host Controller Interface)**
  - Provides a command interface to baseband controller and link manager, also to hardware status, control and event register
  - Bluetooth defined Host Controller Transport Layers
    - UART/RS-232 (HCI over serial interface)
    - USB (HCI over USB interface, e.g., USB dongle)

Bluetooth – Layers

- **L2CAP (Logical Link Control and Adaptation Protocol)**
  - provides a connection-oriented and connectionless service to upper layer
  - protocols with quality-of-service functions using multiplexing, segmentation and reassembly
  - two link types defined in Baseband layer:
    - SCO (synchronous connection-oriented)
    - ACL (asynchronous connection-less) → supported by L2CAP
- **RFCOMM (Radio Frequency Communication)**
  - provides emulation of serial ports, supports up to 60 simultaneous connections
  - Differentiates between two device types
    - Type 1: communication end points (e.g., printer, headsets)
    - Type 2: devices which are part of communication (e.g., modems)

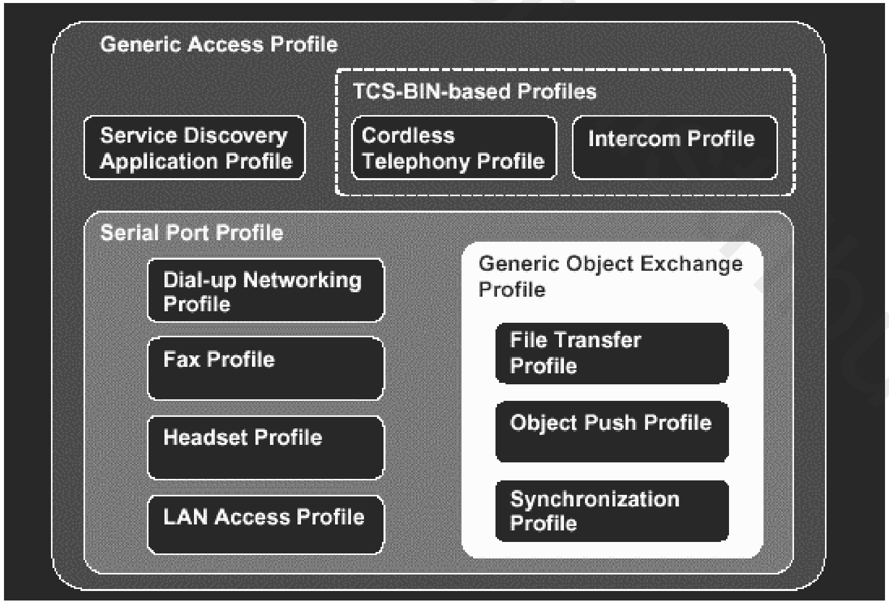
Bluetooth – Layers

- **SDP (Service Discovery Protocol)**
  - discovers which services are available
  - identifies the characteristics of the services
  - uses a request/response model where each transaction consists of one request protocol data unit (PDU) and one response PDU
  - SDP is used with L2CAP
  - is optimized for the dynamic nature of Bluetooth
  - SDP does not define methods for accessing services



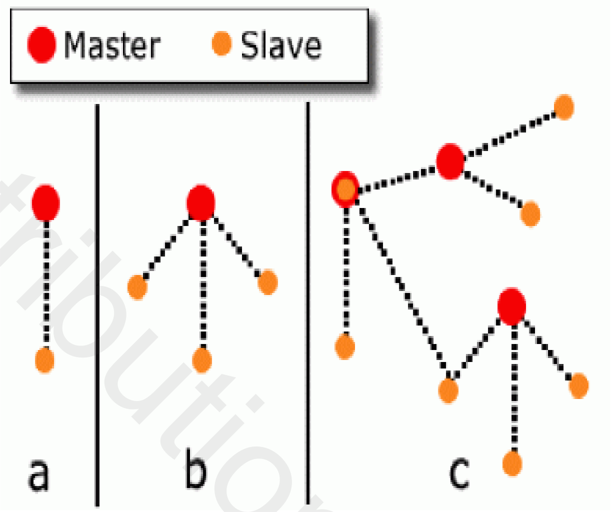
Bluetooth – Layers

- **Profiles**
  - how Bluetooth is used
  - describe how implementations for a specific use must be written
  - defines options in each protocol
  - defines parameter ranges
  - profiles are used to solve interoperability problems between different manufacturers’ products



Bluetooth – Layers

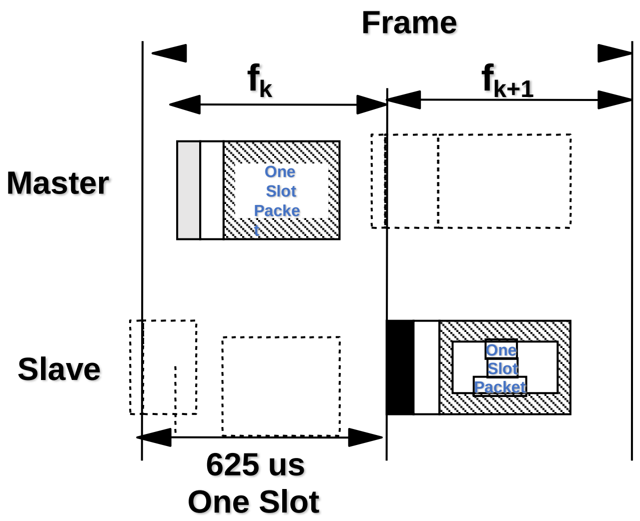
- **Ad-hoc networking**
    - Piconet
        - decentral, one master up to 7 slaves
        - up to 255 parked slaves
        - point-to-point or point-to-multipoint connection
        - unique Bluetooth device address
    - Scatternet
        - overlapping of two piconets, up to 10
        - different hopping sequences
        - P2P network

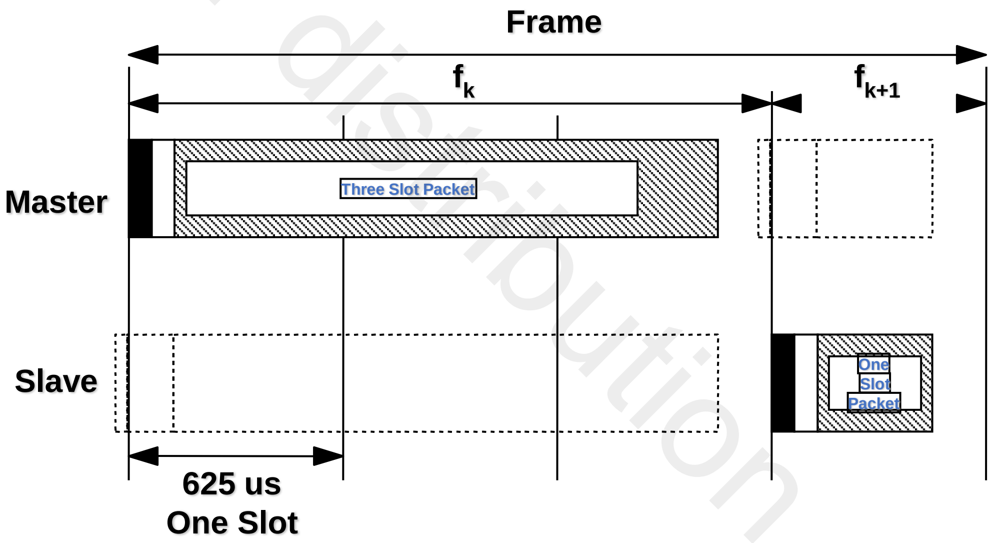


- a: piconet with a single slave
- b: piconet with a multi slave
- c: scatternet

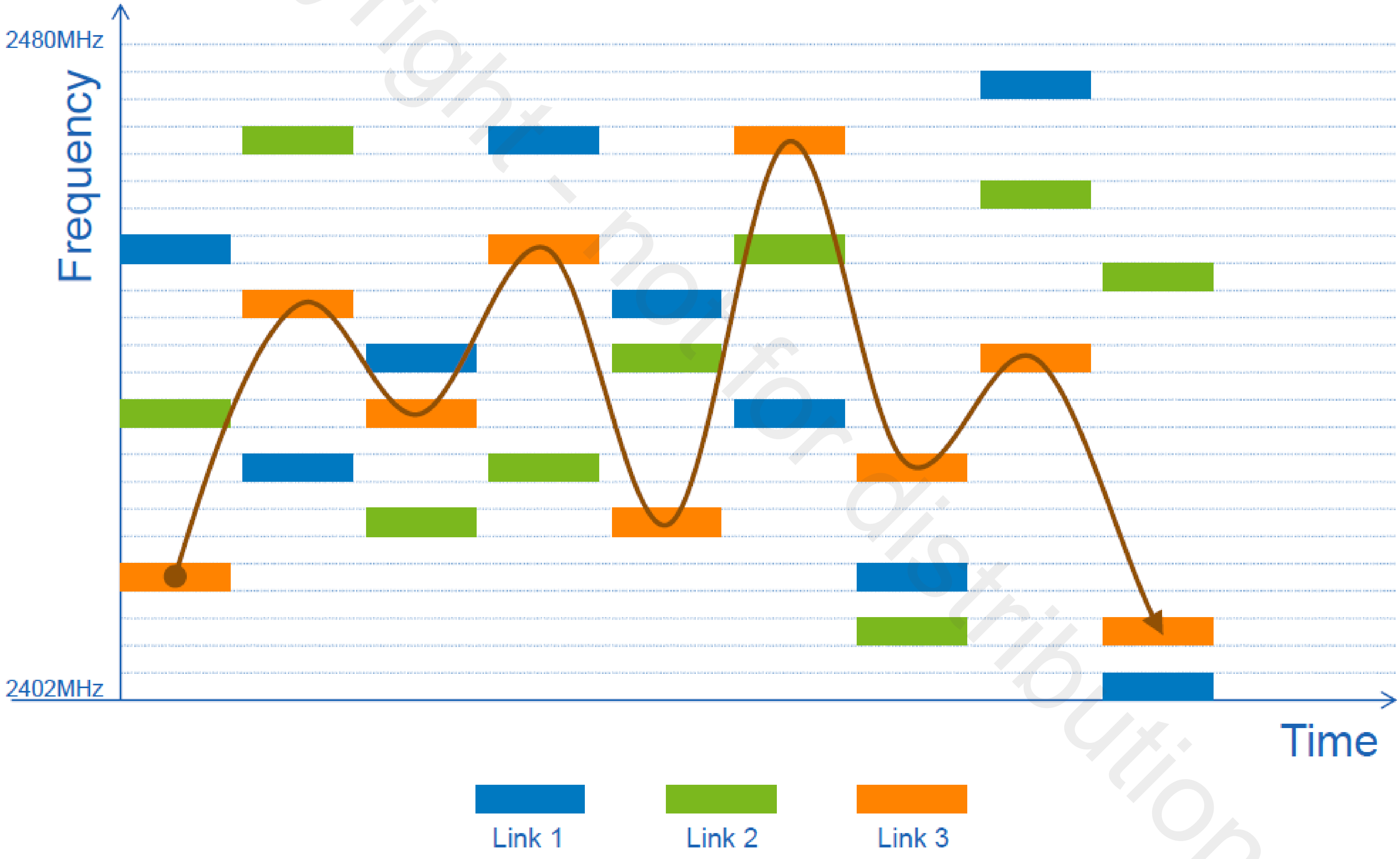
Frequency Hopping Spread Spectrum

- Used to mitigate interference in 2.4 GHz band
- 1,600 hops/second throughout 79 channels (1 MHz each)
- Spreads Bluetooth traffic over the entire ISM band
- All slaves in piconet follow the master for frequency hop sequence
- Hops every packet, packets can be 1,3,5 slots long (625µs/slot)

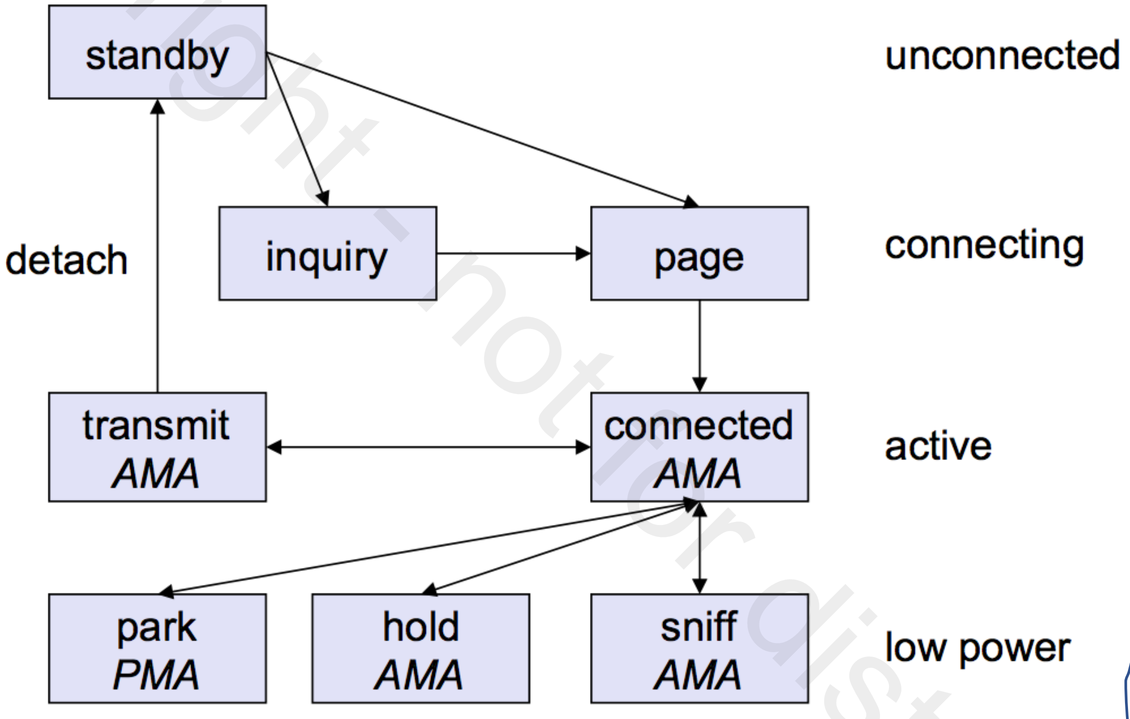




Frequency Hopping Spread Spectrum



Bluetooth States



standby

unconnected

inquiry

page

connecting

detach

transmit
AMA

connected
AMA

active

park
PMA

hold
AMA

sniff
AMA

low power

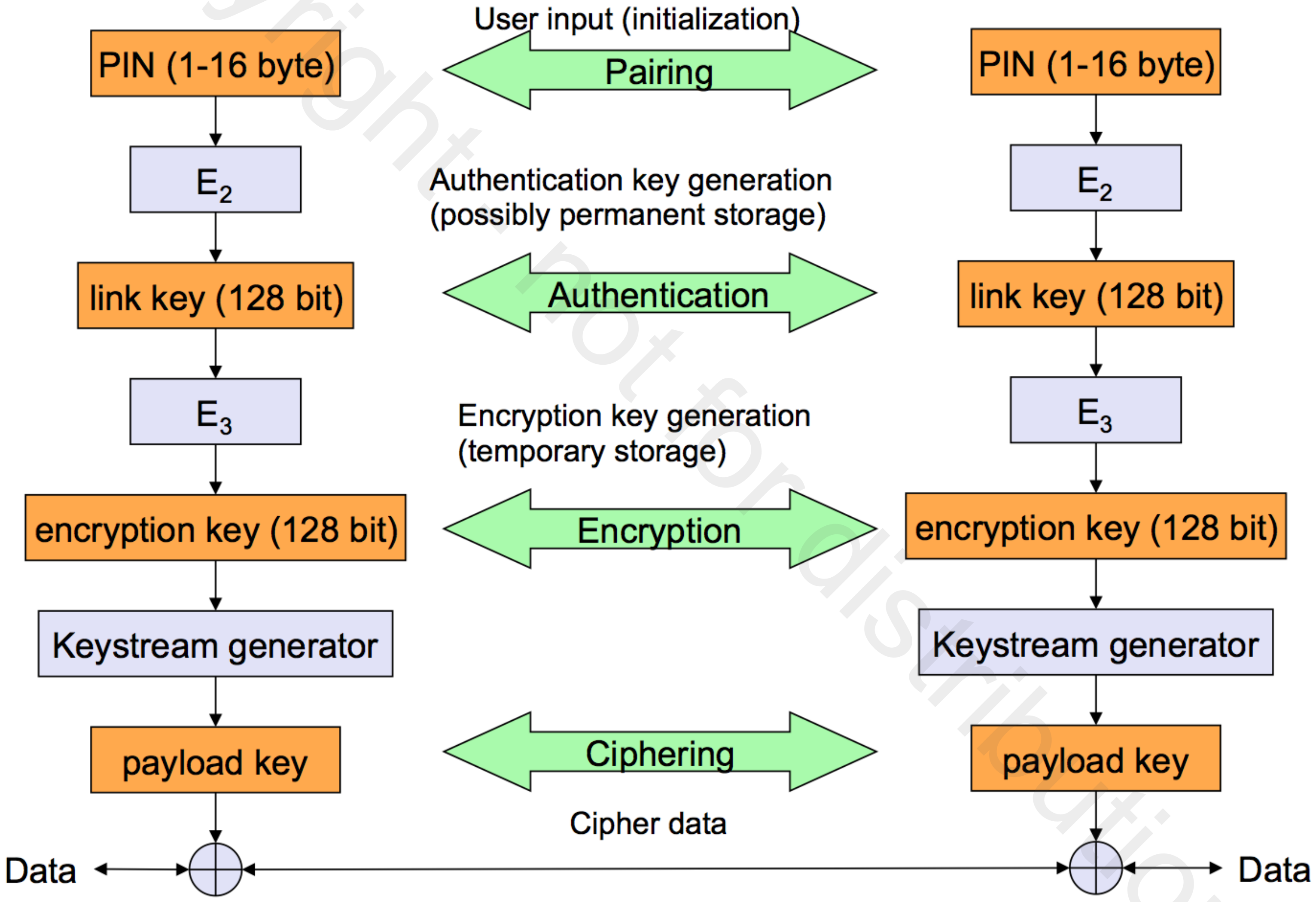
AMA: Active member address

PMA: Parked member address

Standby: do nothing
Inquire: search for other devices
Page: connect to a specific device
Connected: participate in a piconet

Park: release AMA, get PMA
Sniff: listen periodically, not each slot
Hold: stop ACL, SCO still possible, possibly participate in another piconet

Bluetooth Security



Bluetooth Security

- **Pairing**
  - Device pairing is the process of associating two devices each other
  - During the pairing process, identifying information unique to each device is stored in the paired device
  - Can automatically identify each other during future communication sessions after pairing
- **Encryption**
  - Using the link key, an encryption key is created, used to modify(encrypt) user data for privacy
  - Encryption key used for Bluetooth communication sessions changes with each new session

ZigBee

- One of the most popular industry wireless mesh networking standards for connecting sensors, instrumentation and control systems
- Open, global, packet-based protocol
- Designed to provide easy-to-use architecture for secure, reliable, low power wireless networks
- IEEE 802.15.4 standard was first completed in 2003
- ZigBee Alliance was established in 2002
- ZigBee enhances the IEEE 802.15.4 standard
  - providing a simple networking layer and standard application profiles
  - interoperable multi-vendor consumer electronic solution

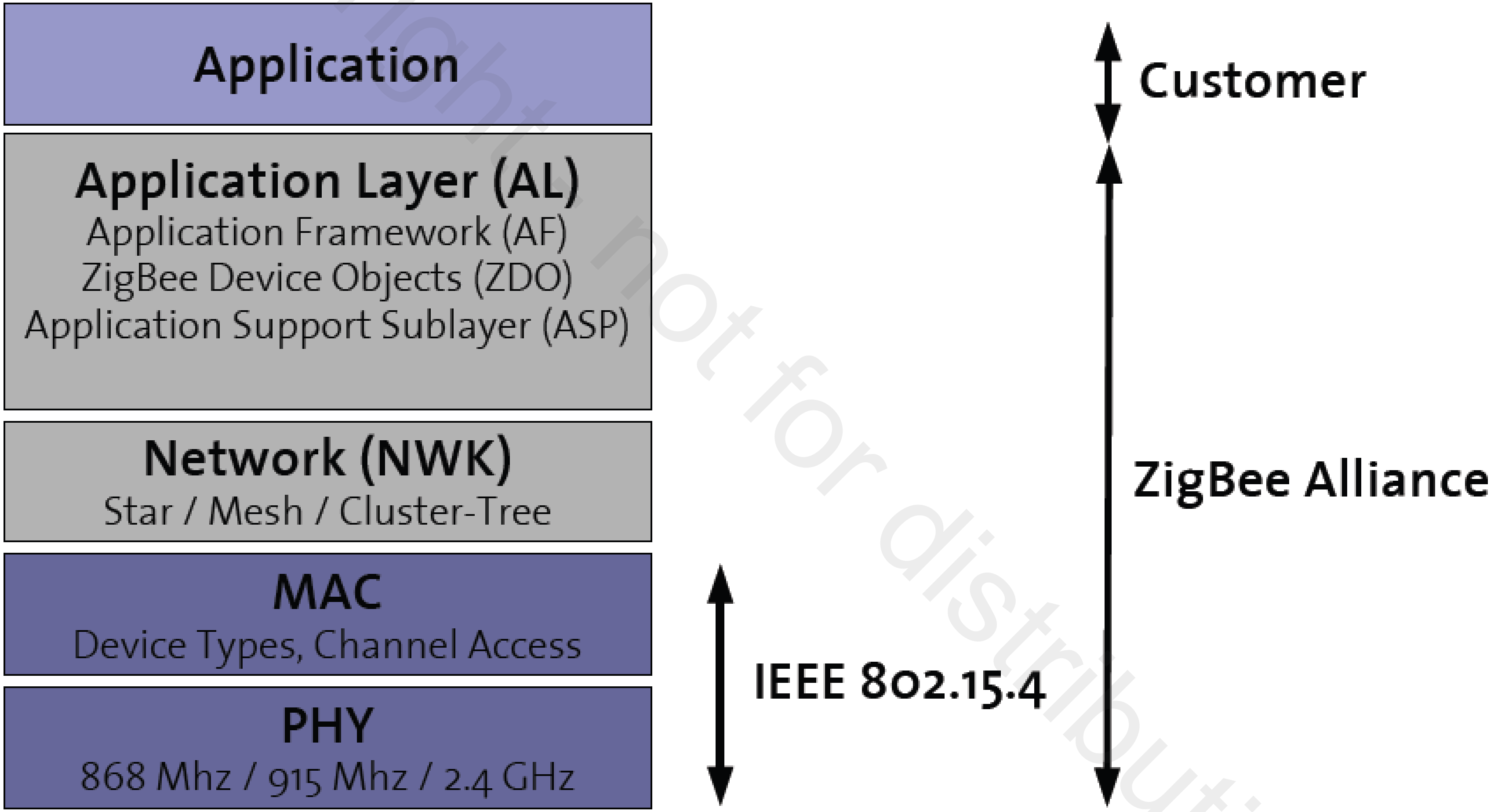
ZigBee

- **Industrial and Commercial**
  - Monitors
  - Movement Sensors
  - Automation
- **Personal Healthcare**
  - Patient monitors
  - Remote Diagnosis
  - Data loggers
- **Building Automation**
  - Security
  - Lighting
  - Fire and Safety systems
- **Automotive**
  - Service controls
  - Inventory tracking

ZigBee

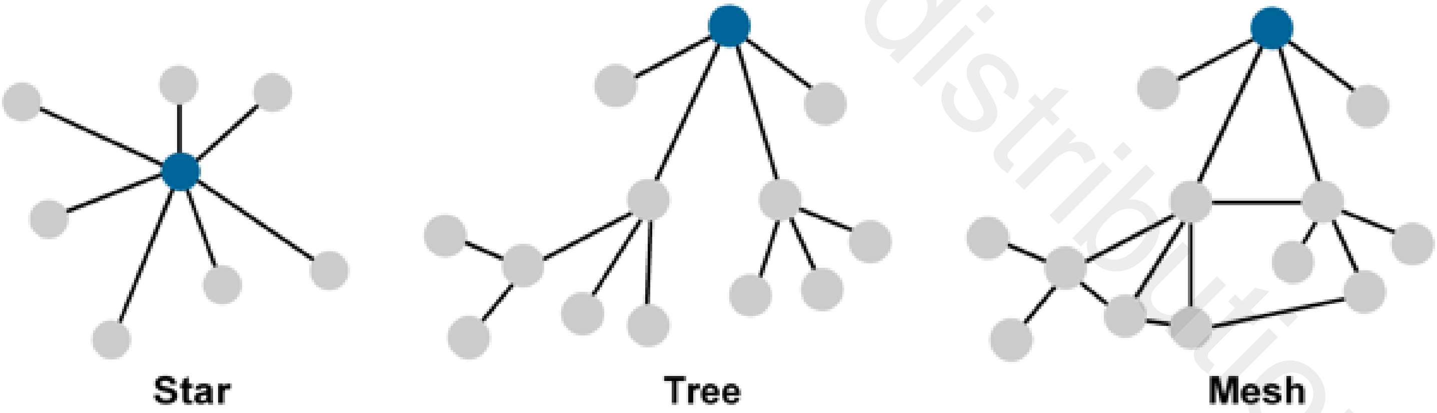
- Low power consumption and simply implemented
- Users expect batteries to last many months to years
  - allow batteries to last up to years using primary cells without any charging process
- High density of nodes per network
  - Uses IEEE 802.15.4 PHY and MAC layers
  - Allows networks to handle any number of devices
- ZigBee/IEEE 802.15.4 has active (transmit/receive) or sleep modes
  - Bluetooth has many different modes, states depending upon your latency and power requirements (sniff, park, hold, active, etc..)
- ZigBee's protocol code stack is about ¼ of Bluetooth's stack
  - Essential to cost, interoperability and maintenance

ZigBee Protocol Stack


Application
Application Layer (AL)
Application Framework (AF)
ZigBee Device Objects (ZDO)
Application Support Sublayer (ASP)
Network (NWK)
Star / Mesh / Cluster-Tree
MAC
Device Types, Channel Access
PHY
868 Mhz / 915 Mhz / 2.4 GHz
Customer
ZigBee Alliance
IEEE 802.15.4

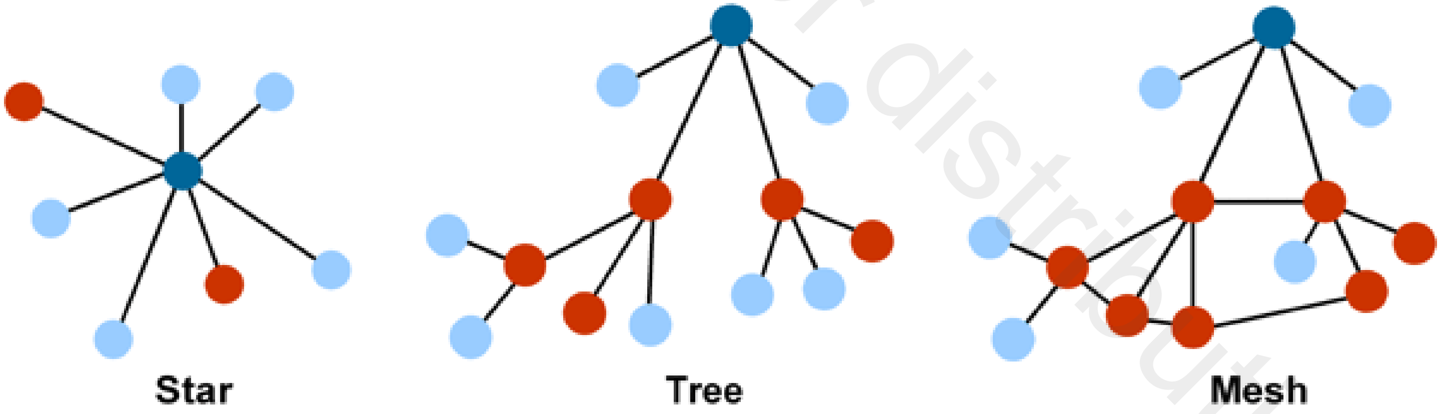
ZigBee Network and Device Types

- **Coordinator (Full Function Device: FFD)**
  - Responsible for overall network management
  - Assigns how addresses are allocated to nodes or routers
  - Permits other devices to join/leave the network
  - Holds a list of neighbors and routers, transfers application packets
  - Equivalent of access point in Wi-Fi or master in Bluetooth



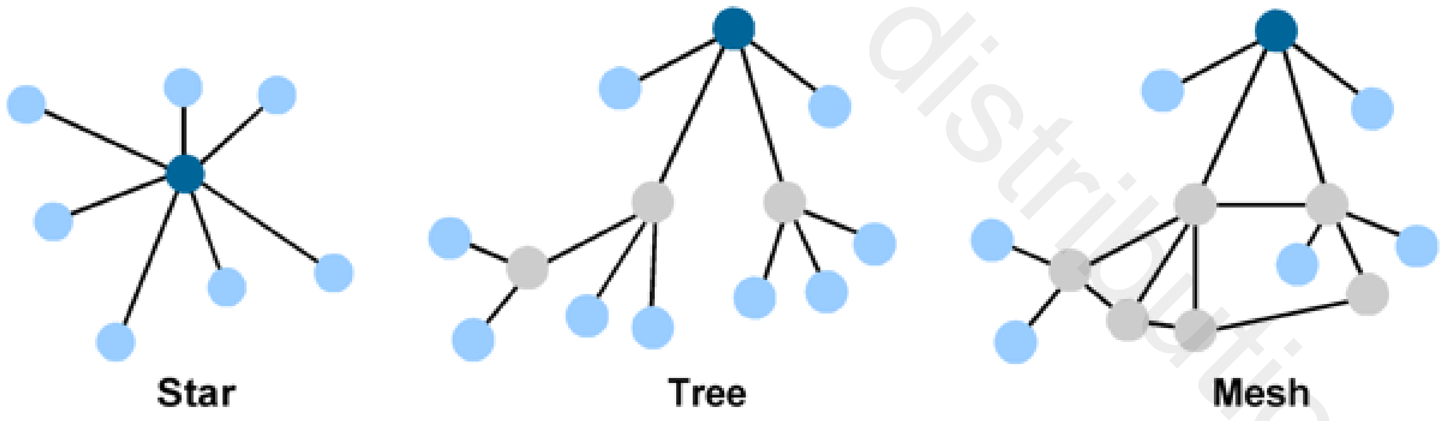
ZigBee Network and Device Types

- **Router (Full Function Device: FFD)**
  - Used in tree and mesh topologies to expand network coverage
  - Not necessary in a star network (coordinator can be the router)
  - Performs all functions similar to a coordinator except establishing of a network

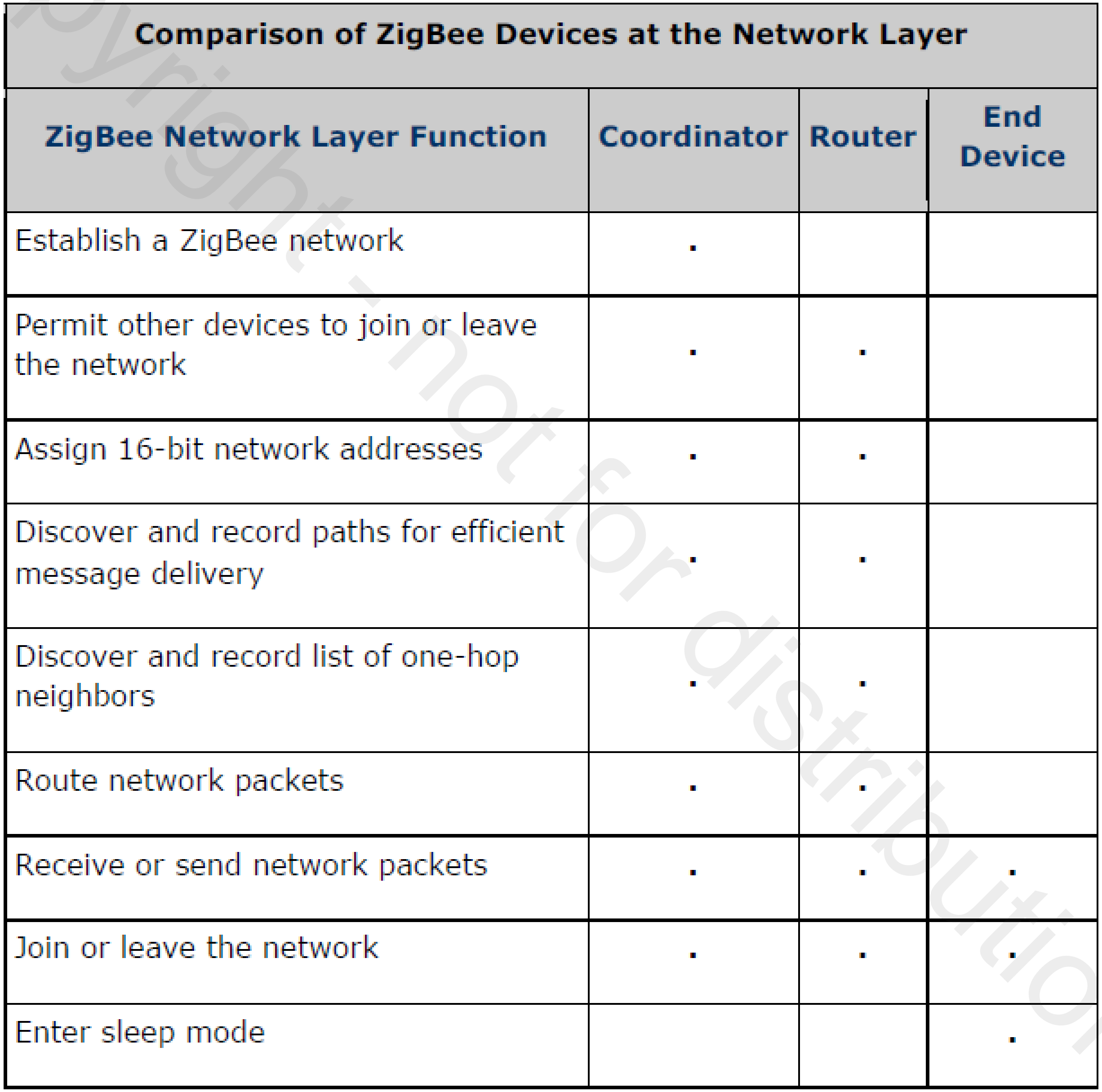


ZigBee Network

- **End Device (Reduced Function Device: RFD)**
  - Operates within a limited set of IEEE 802.15.4 MAC layer (less power)
  - End device can be connected to a router or coordinator
  - Consumes power only when transmitting information
  - Can only send and receive, cannot relay messages
  - In star topology, they are perimeter nodes
  - In tree and mesh topology, they are leaf nodes



ZigBee Network



Comparison of ZigBee Devices at the Network Layer

ZigBee Network Layer Function	Coordinator	Router	End Device
Establish a ZigBee network	•		
Permit other devices to join or leave the network	•	•	
Assign 16-bit network addresses	•	•	
Discover and record paths for efficient message delivery	•	•	
Discover and record list of one-hop neighbors	•	•	
Route network packets	•	•	
Receive or send network packets	•	•	•
Join or leave the network	•	•	•
Enter sleep mode			•

Bluetooth vs ZigBee

Features	ZigBee	Bluetooth
Standard	IEEE 802.15.4	IEEE 802.15.1
Topology	Mesh, Star, Tree	Star
Data Rate	250 Kbps	1 Mbps
Nodes	65,000	7 slaves, 1 master
Power Profile	Very Low (Months ~ Years)	Low (Days ~ Weeks)
Range	100m+ (984ft)	10m (32ft)
Complexity	Simple	Complex

ZigBee Addressing

- IEEE 802.15 compliant radio has a 64-bit address (MAC address)
    - All are unique, obtained from IEEE to ensure global uniqueness
- When the device joins a ZigBee network, it receives a 16-bit “network” address
    - 2^16 = 65,536 devices can be connected to a ZigBee network
- Either a 64-bit address (MAC) or a 16-bit “network” address/ID can be used within the PAN to communicate with a device
    - Coordinator always has a “network” address/ID of 0
    - “network” address/ID assigned dynamically

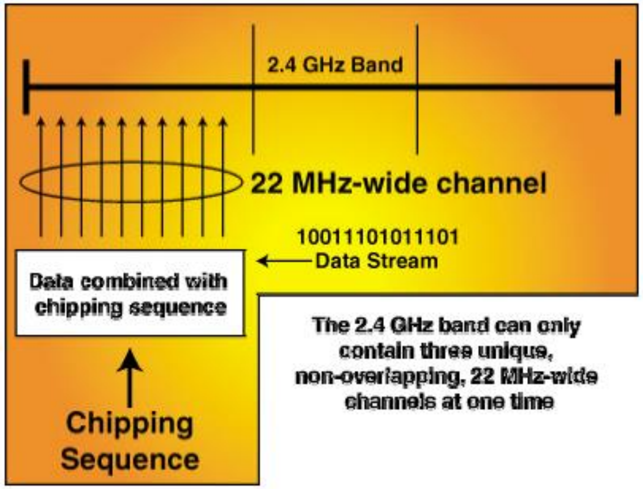
Coexistence – Bluetooth and ZigBee

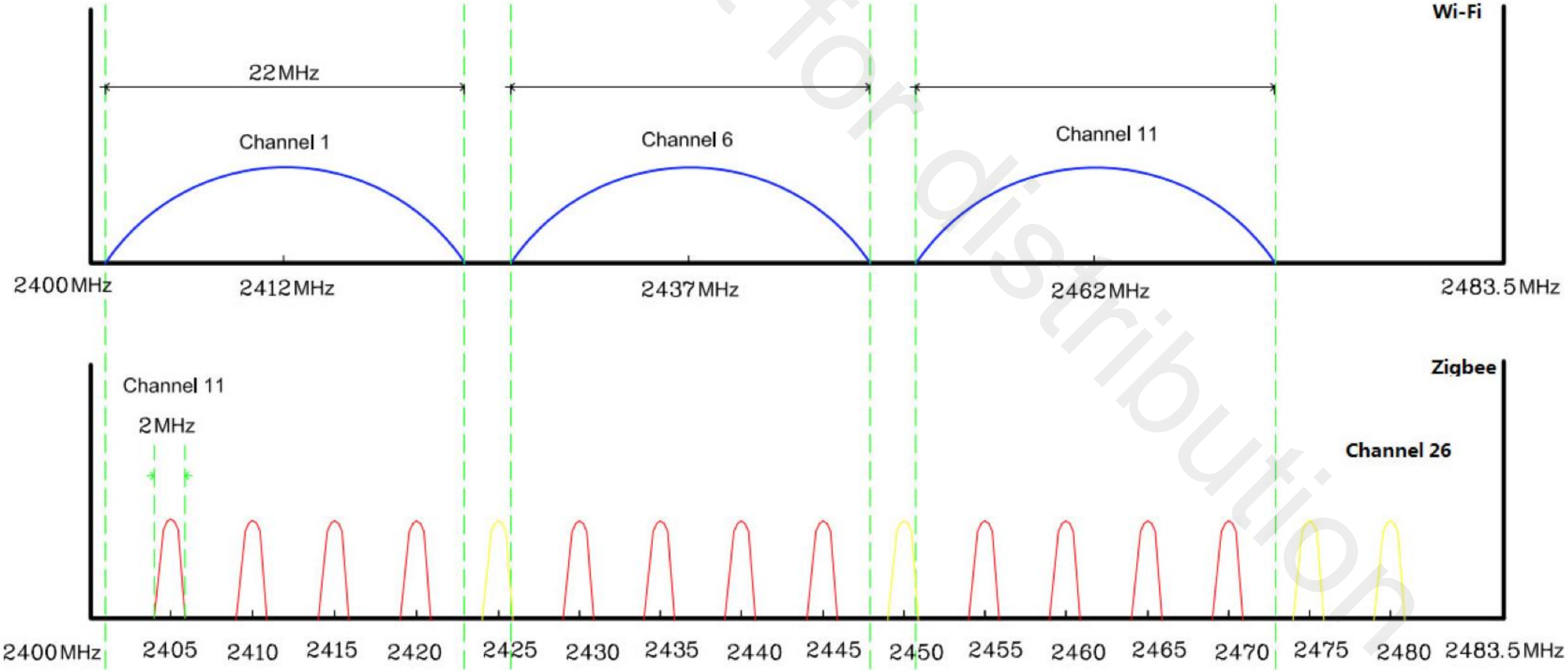
- Bluetooth is FHSS (frequency hopping spread spectrum)
  - Its working frequency quickly hops 1600 times per second
  - Even if there are several kinds of 2.4GHz RF systems, the hopping system only interferes with other RF systems for a short period of time
- ZigBee is DSSS (direct sequence spread spectrum)
  - Only one time channel overlap in 79 times with Bluetooth
  - If a Bluetooth device transmits in a frequency that overlaps with the ZigBee channel, then the ZigBee device randomly backs off while the Bluetooth quickly hops to another frequency

- **Thus, Bluetooth and ZigBee rarely disturb each other, and can co-exist well.**

Coexistence – Wi-Fi and ZigBee

- Both are DSSS
  - The interference in Wi-Fi caused by ZigBee is smaller than the interference in ZigBee caused by Wi-Fi
  - ZigBee's bandwidth (2MHz) is much smaller than Wi-Fi's bandwidth (22MHz)


2.4 GHz Band
22 MHz-wide channel
10011101011101
Data Stream
Data combined with chipping sequence
Chipping Sequence
The 2.4 GHz band can only contain three unique, non-overlapping, 22 MHz-wide channels at one time



NFC

- Near Field Communication
  - Data Exchange, simplified transaction
  - Passive Electronic Tag
  - Short-range 13.56MHz P2P
- Builds on specifications laid out for earlier RFID technology
- Tag-on-demand Android application
- Bluetooth Connection Handover
  - Eliminating manual pairing process
- Setup time is less than 0.1sec, power consumption is less than 15mA
- Possible transfer rates
  - 106, 212, 424 kbps

Comparison of Wireless Technologies

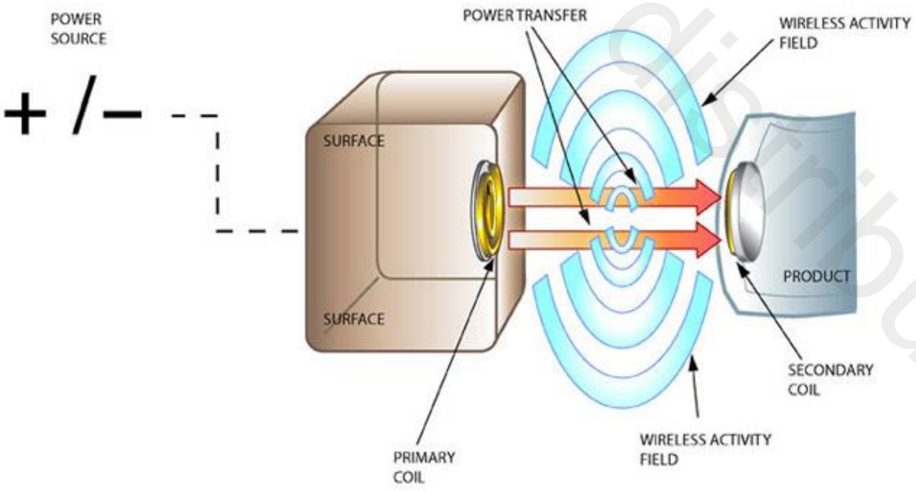
	NFC	RFID	Bluetooth	Wi-Fi
Maximum Operating Range	10 cm	3 m	100 m	100 m
Operating Frequency	13.56 MHz	Varies	2.4 GHz	2.4/5 GHz
Directional Communication	Two way	One way	Two way	Two way
Bit Rate	106/212/ 424 Kbps	Varies	22 Mbps	144 Mbps
Potential Uses	e-Tickets, Credit card payment, Membership card	Tracking items, EZ-Pass	Communicate between phones, peripheral devices	Wireless internet

NFC Applications

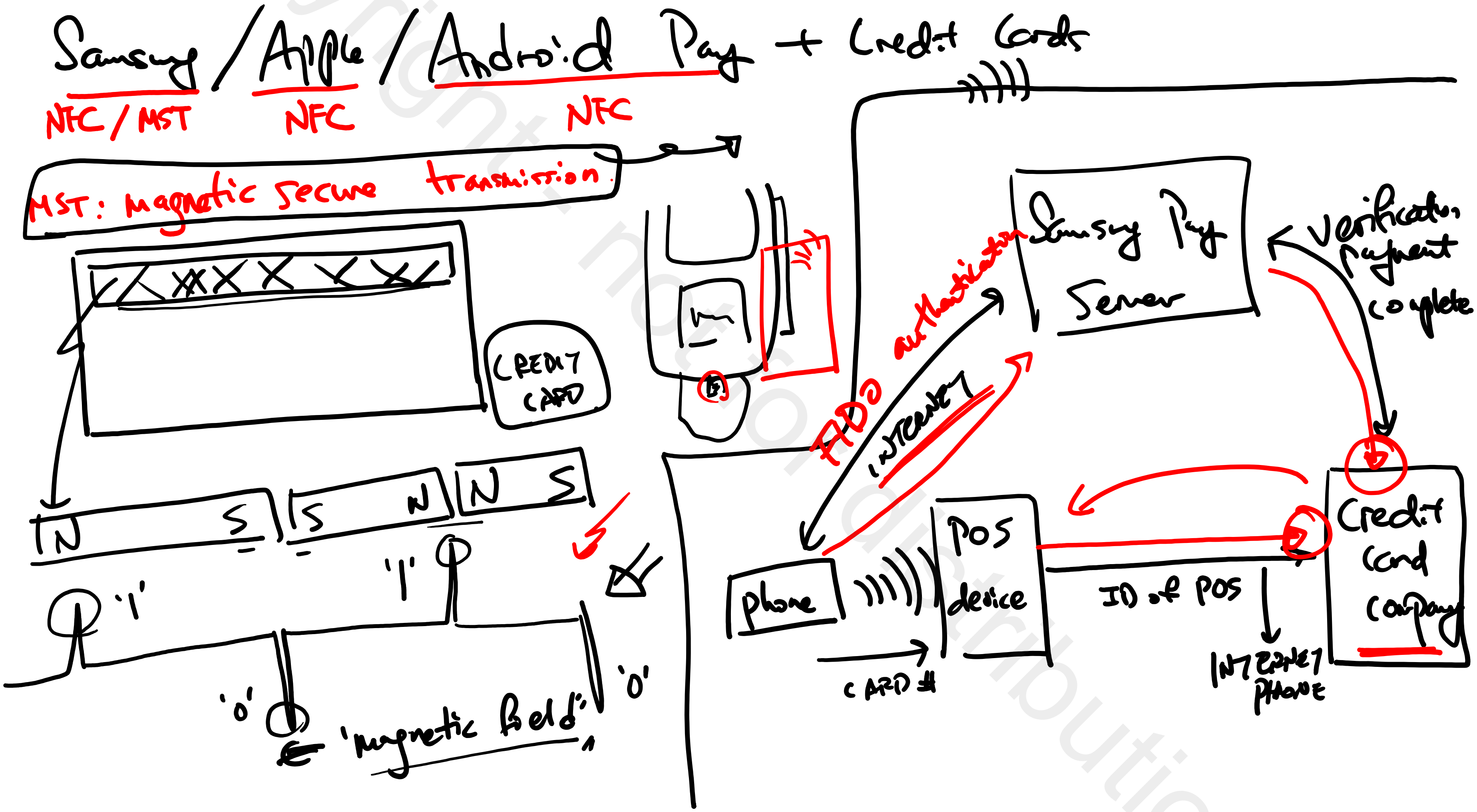
	Bus/Train Station, Airport	Vehicle	Office	Store, Restaurant	Theater, Stadium	Anywhere
Usage of NFC Mobile Phone	Ticketing Get information from smart poster Get information from info kiosk Pay bus/taxi fare	Adjust seat position Open door Pay parking fees	Enter/exit office building Exchange business cards Log into PC Print using copier machine	Pay by credit card Get loyalty points Get and use coupons Share information and coupon among users	Electronic ticket Get event information	Download and personalize application Check usage history Download ticket Lock phone remotely
Service Industries	Mass transport Advertising	Public transport	Security	Banking Retail Credit Card	Entertainment	Any

NFC – Inductive Coupling

- Induction is the production of electric current by passing a wire through a magnetic field
- NFC devices have coils built into them. A magnetic field from an NFC device generates power in these coils, which initiates the transmission of data into radio waves
- Both devices share this power



Samsung/Apple/Android Pay


Samsung / Apple / Android Pay + Credit Cards
NFC / MST
NFC
NFC
MST: magnetic secure transmission
CREDIT CARD
N
S
S
N
N
S
'1'
'1'
'0'
'0'
'magnetic field'
Samsung Pay Server
verification payment complete
FIDO authentication
INTERNET
Phone
POS device
CARD #
ID of POS
INTERNET PHONE
Credit Card Company