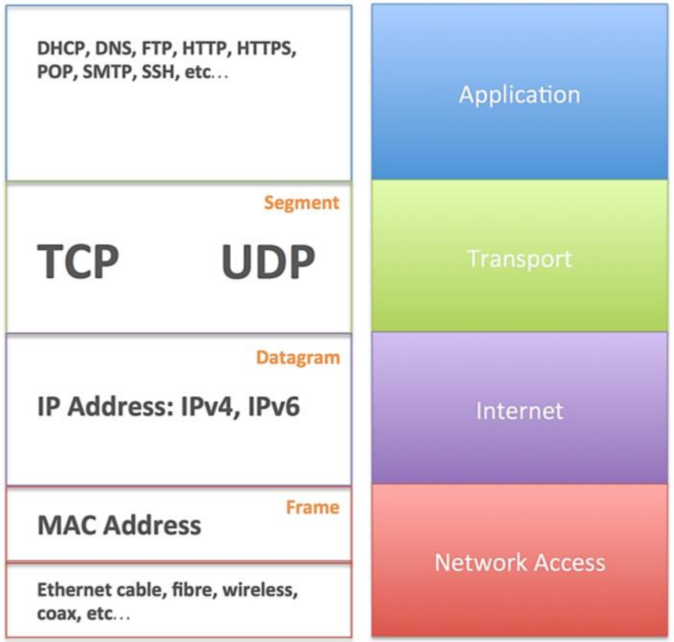
Ch. 9 - IoT Requirements for Networking Protocols

COMPSCI 147

Internet-of-Things; Software and Systems

Recall: TCP/IP protocol stack (Internet Protocol stack)



Layered abstractions

- Hide implementation details from layer above or below

Normalization (IP) layer

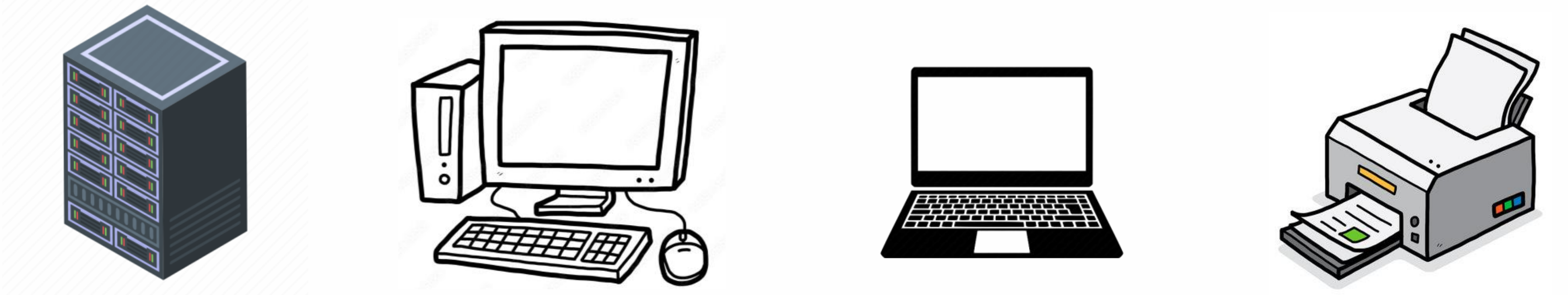
- Enables system interoperability while accommodating different network access technologies

Challenge 1: Support for Constrained Devices

- Traditional internet:

Challenge 1: Support for Constrained Devices

- Traditional internet:



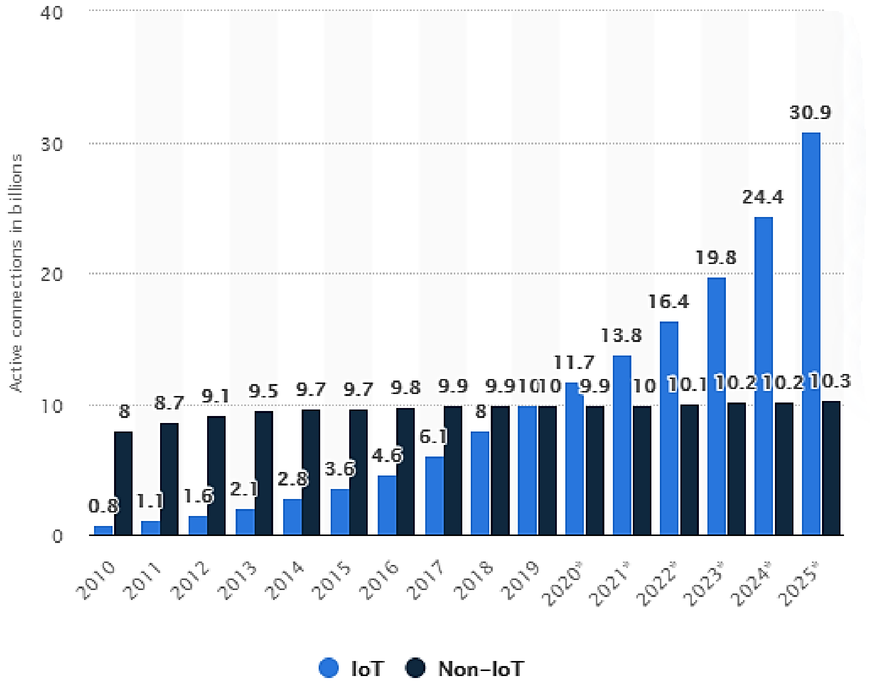
- With IoT

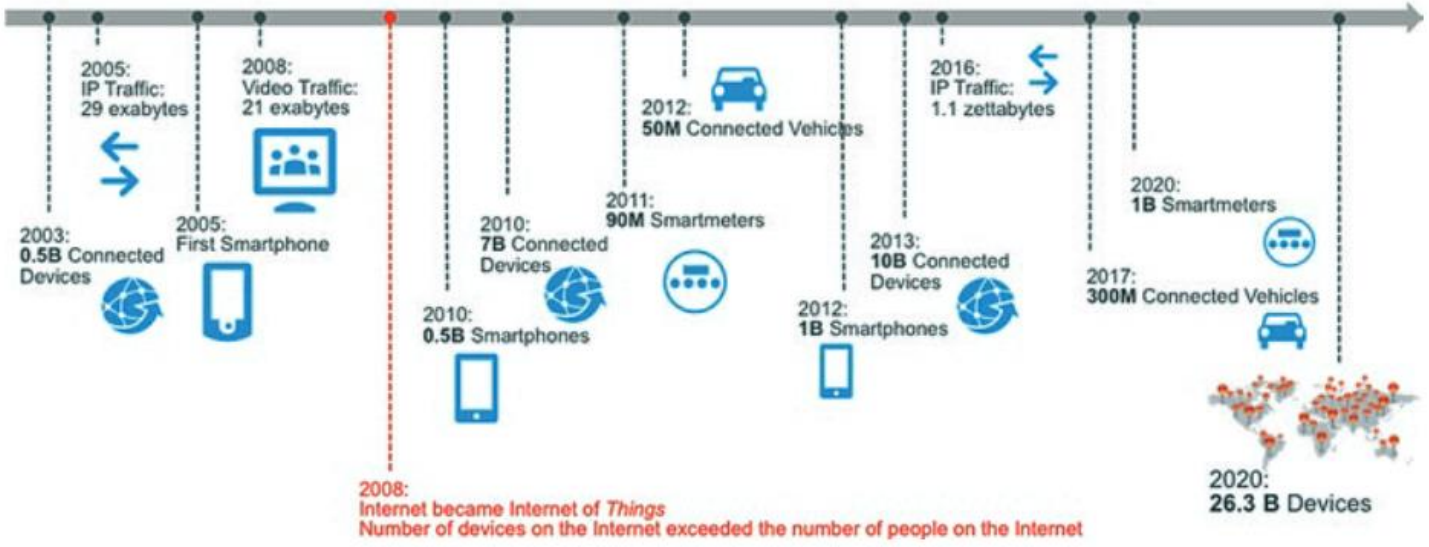
Limited Processor Speed

Constrained Memory

Low Power

Challenge 2: Massive Scalability





2003: 0.5B Connected Devices
2005: IP Traffic: 29 exabytes
2005: First Smartphone
2008: Video Traffic: 21 exabytes
2008: Internet became Internet of Things
Number of devices on the Internet exceeded the number of people on the Internet
2010: 0.5B Smartphones
2010: 7B Connected Devices
2011: 90M Smartmeters
2012: 50M Connected Vehicles
2012: 1B Smartphones
2013: 10B Connected Devices
2016: IP Traffic: 1.1 zettabytes
2017: 300M Connected Vehicles
2020: 1B Smartmeters
2020: 26.3 B Devices

Challenge 2: Massive Scalability

- Device Addressing
- Credentials Management
- Control Plane
- Wireless Spectrum

- Internet traditionally used IPV4 address
- 32-bit address (e.g., 192.0.1.246)
- Maximum devices supported: 4.3 billion!

- IoT devices should be individually addressable for ubiquitous communication.
- Fallback: Gateways or proxys.

Challenge 2: Massive Scalability

Device Addressing

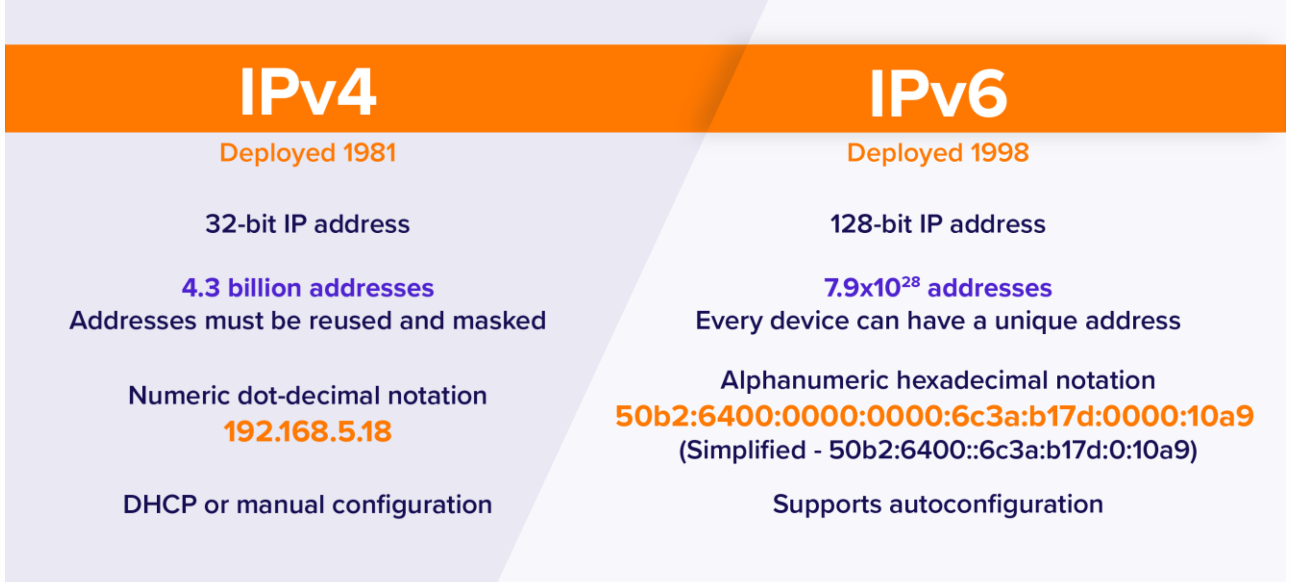
Credentials Management

Control Plane

Wireless Spectrum

- Internet traditionally used IPV4 address
- 32-bit address (e.g., 192.0.1.246)
- Maximum devices supported: 4.3 billion!

- IoT devices should be individually addressable for ubiquitous communication.
- Fallback: Gateways or proxys.



IPv4	IPv6
Deployed 1981	Deployed 1998
32-bit IP address	128-bit IP address
4.3 billion addresses Addresses must be reused and masked	7.9x10^{28} addresses Every device can have a unique address
Numeric dot-decimal notation 192.168.5.18	Alphanumeric hexadecimal notation 50b2:6400:0000:0000:6c3a:b17d:0000:10a9 (Simplified - 50b2:6400::6c3a:b17d:0:10a9)
DHCP or manual configuration	Supports autoconfiguration

Challenge 2: Massive Scalability

- Impossible to pre-configure sheer number of devices
- Lack user-interface on constrained device..

- Device Addressing
- Credentials Management
- Control Plane
- Wireless Spectrum

- Requirements for IoT:
  - Lightweight
  - No/low-touch
  - Highly automated credentials management mechanisms

Challenge 2: Massive Scalability

Device Addressing

Credentials Management

Control Plane

Wireless Spectrum

For instance,

You have developed a ESP32 based smart-product without any user interface.
Develop a solution for users to connect it to WiFi without hardcoding credentials in code..

Challenge 2: Massive Scalability

Device Addressing

Credentials Management

Control Plane

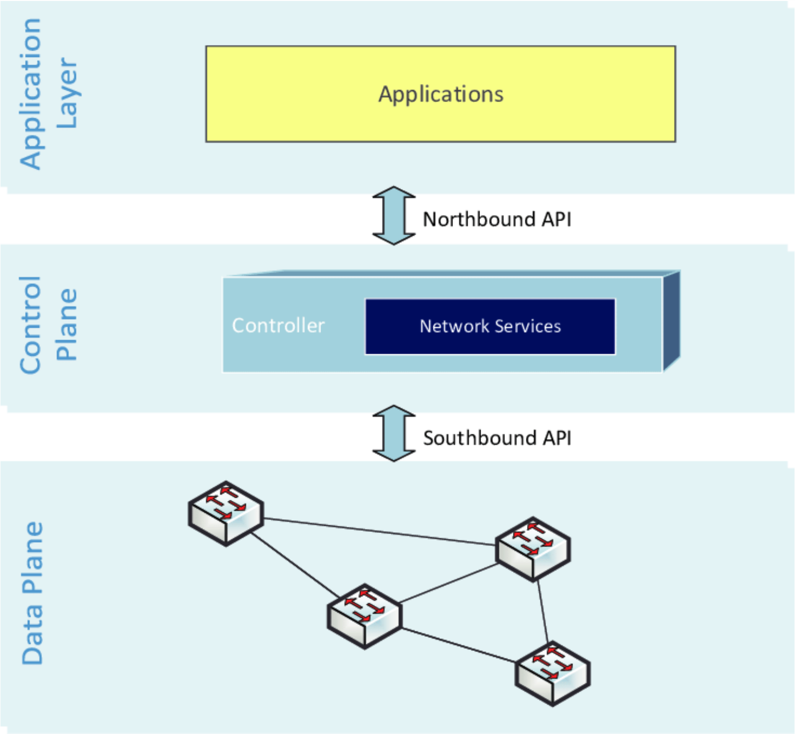
Wireless Spectrum

Control plane protocols:

- Discovers topology information
- Communicating connectivity status or link health
- Signaling session or connection state
- Guaranteeing quality of service
- Quickly reacting to faults.

Data plane protocols:

- transfers the actual message.

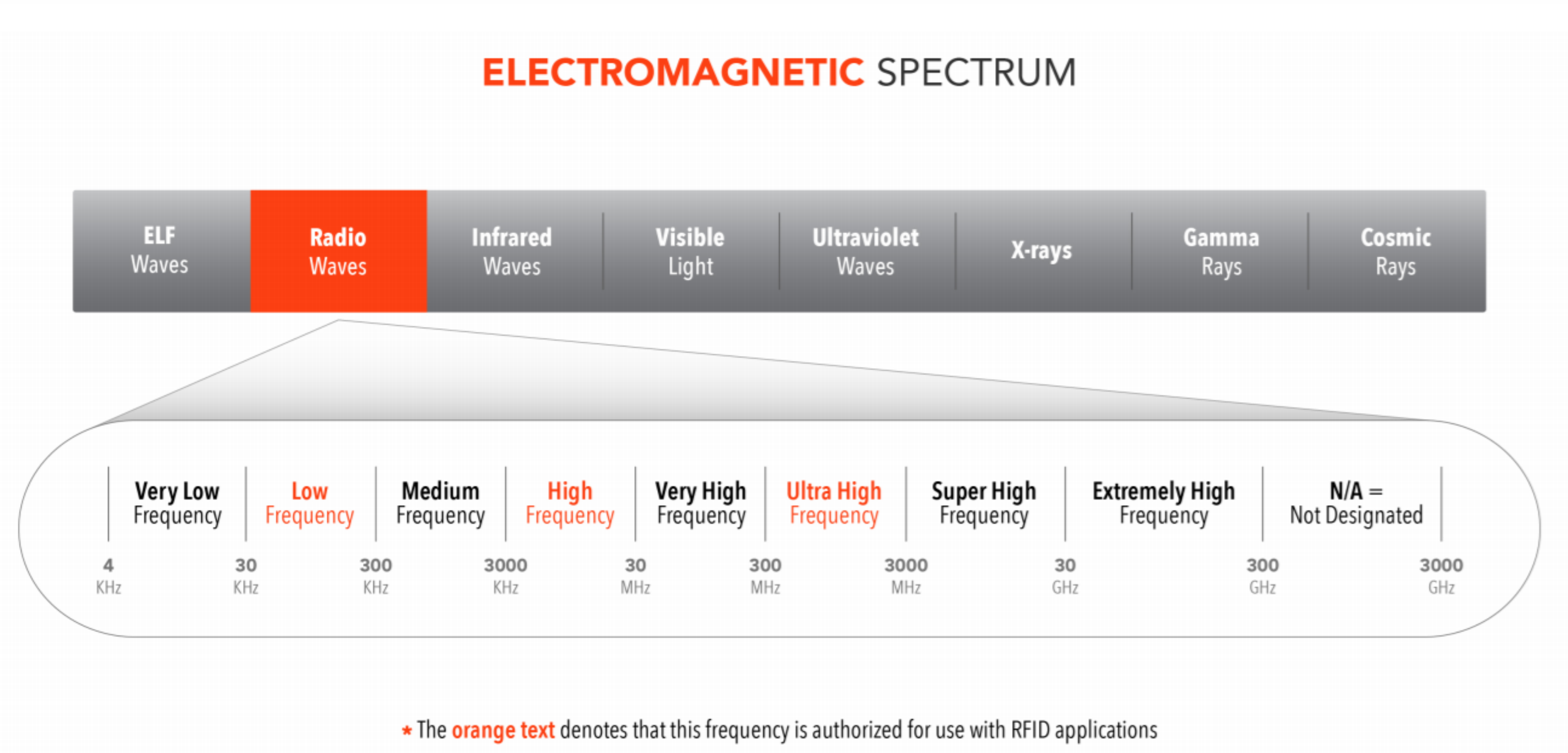


Scalability of IoT devices requires an elastic control plane

Challenge 2: Massive Scalability

the hottest real estate market may be one we can’t see.

- Device Addressing
- Credentials Management
- Control Plane
- Wireless Spectrum

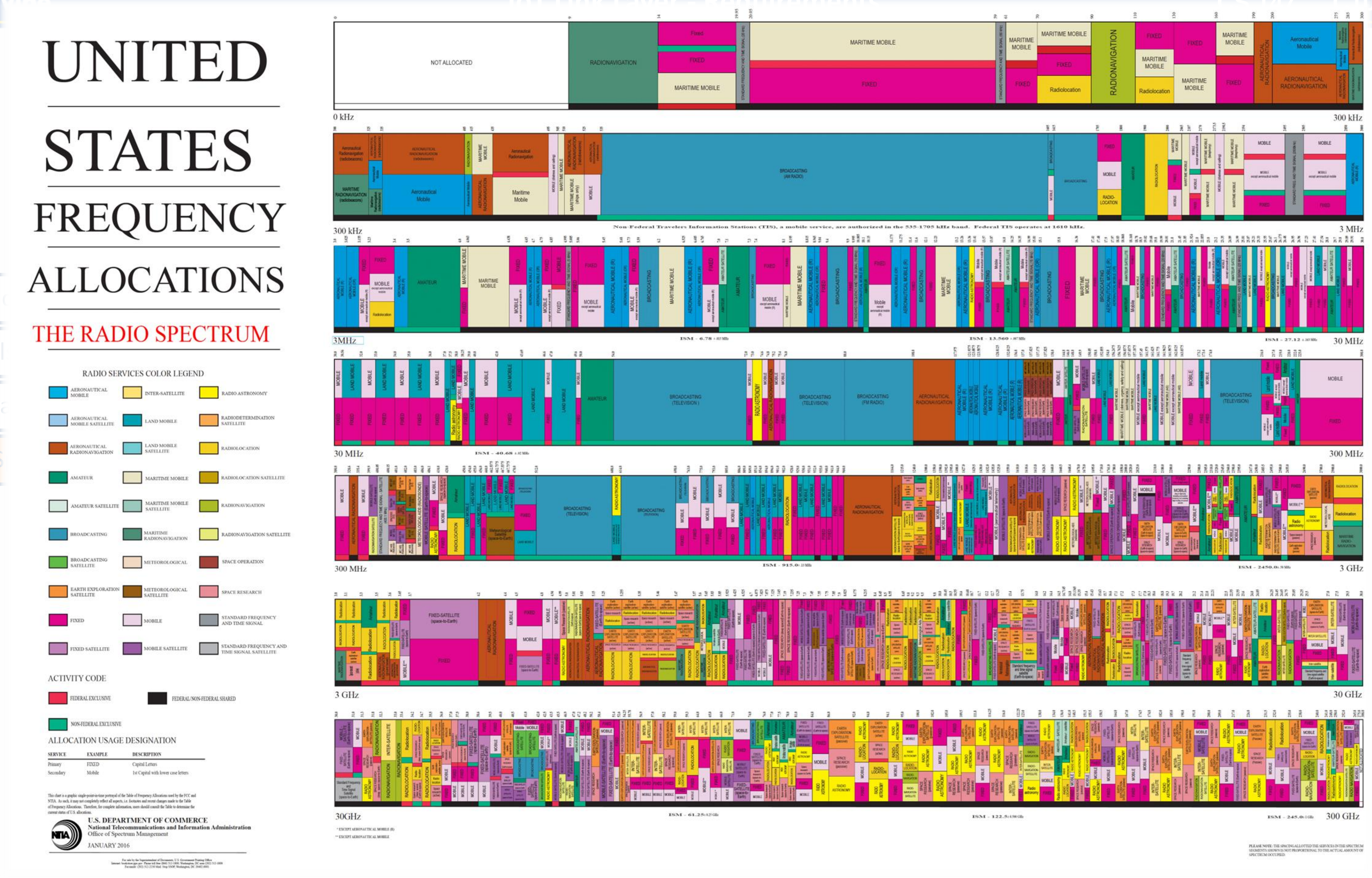


UC Ir

IoT Link Layer - Requirements

CS 147 … C10_01_12

- Device Ad
- Credential
- Control Pl
- Wireless S



UNITED STATES FREQUENCY ALLOCATIONS

THE RADIO SPECTRUM

RADIO SERVICES COLOR LEGEND

- AERONAUTICAL MOBILE
- INTER-SATELLITE
- RADIO ASTRONOMY
- AERONAUTICAL MOBILE SATELLITE
- LAND MOBILE
- RADIODETERMINATION SATELLITE
- AERONAUTICAL RADIONAVIGATION
- LAND MOBILE SATELLITE
- RADIOLOCATION
- AMATEUR
- MARITIME MOBILE
- RADIOLOCATION SATELLITE
- AMATEUR SATELLITE
- MARITIME MOBILE SATELLITE
- RADIONAVIGATION
- BROADCASTING
- MARITIME RADIONAVIGATION
- RADIONAVIGATION SATELLITE
- BROADCASTING SATELLITE
- METEOROLOGICAL
- SPACE OPERATION
- EARTH EXPLORATION SATELLITE
- METEOROLOGICAL SATELLITE
- SPACE RESEARCH
- FIXED
- MOBILE
- STANDARD FREQUENCY AND TIME SIGNAL
- FIXED SATELLITE
- MOBILE SATELLITE
- STANDARD FREQUENCY AND TIME SIGNAL SATELLITE

ACTIVITY CODE

- FEDERAL EXCLUSIVE
- FEDERAL/NON-FEDERAL SHARED
- NON-FEDERAL EXCLUSIVE

ALLOCATION USAGE DESIGNATION

SERVICE	EXAMPLE	DESCRIPTION
Primary	FIXED	Capital Letters
Secondary	Mobile	1st Capital with lower case letters

This chart is a graphic single-point-in-time portrayal of the Table of Frequency Allocations used by the FCC and NTIA. As such, it may not completely reflect all aspects, i.e. footnotes and recent changes made to the Table of Frequency Allocations. Therefore, for complete information, users should consult the Table to determine the current status of U.S. allocations.

U.S. DEPARTMENT OF COMMERCE
National Telecommunications and Information Administration
Office of Spectrum Management

JANUARY 2016

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone toll free (866) 512-1800; Washington, DC area (202) 512-1800
Facsimile: (202) 512-2250 Mail: Stop SSOP, Washington, DC 20402-0001

Non-Federal Travelers Information Stations (TIS), a mobile service, are authorized in the 535-1705 kHz band. Federal TIS operates at 1610 kHz.

* EXCEPT AERONAUTICAL MOBILE (R)

** EXCEPT AERONAUTICAL MOBILE

PLEASE NOTE: THE SPACING ALLOTTED THE SERVICES IN THE SPECTRUM SEGMENTS SHOWN IS NOT PROPORTIONAL TO THE ACTUAL AMOUNT OF SPECTRUM OCCUPIED.

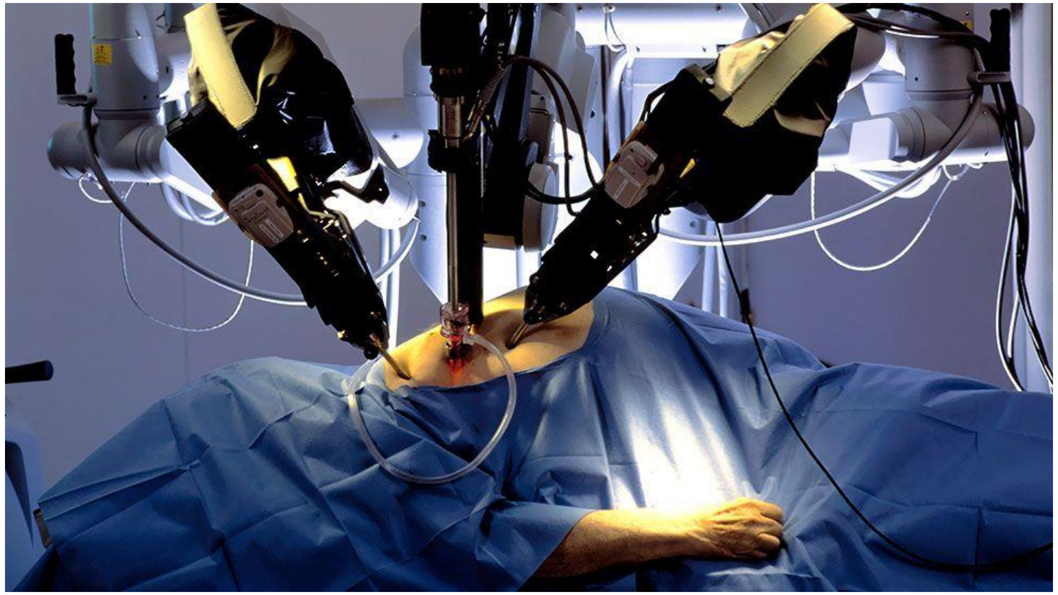
Challenge 2: Massive Scalability

- Device Addressing
- Credentials Management
- Control Plane
- Wireless Spectrum

Spectrum Crunch caused by:

- Growth in the number of endpoints
- Growth in the volume of traffic per endpoint

Challenge 3: Determinism



IoT opens the door for mission-critical use cases with network requirements for real-time response as well as overall network, protocol, and device robustness.

Challenge 3: Determinism

- To support real-time information transfer:
  The time it takes for each packet to traverse a path from its source to its destination should be determined.

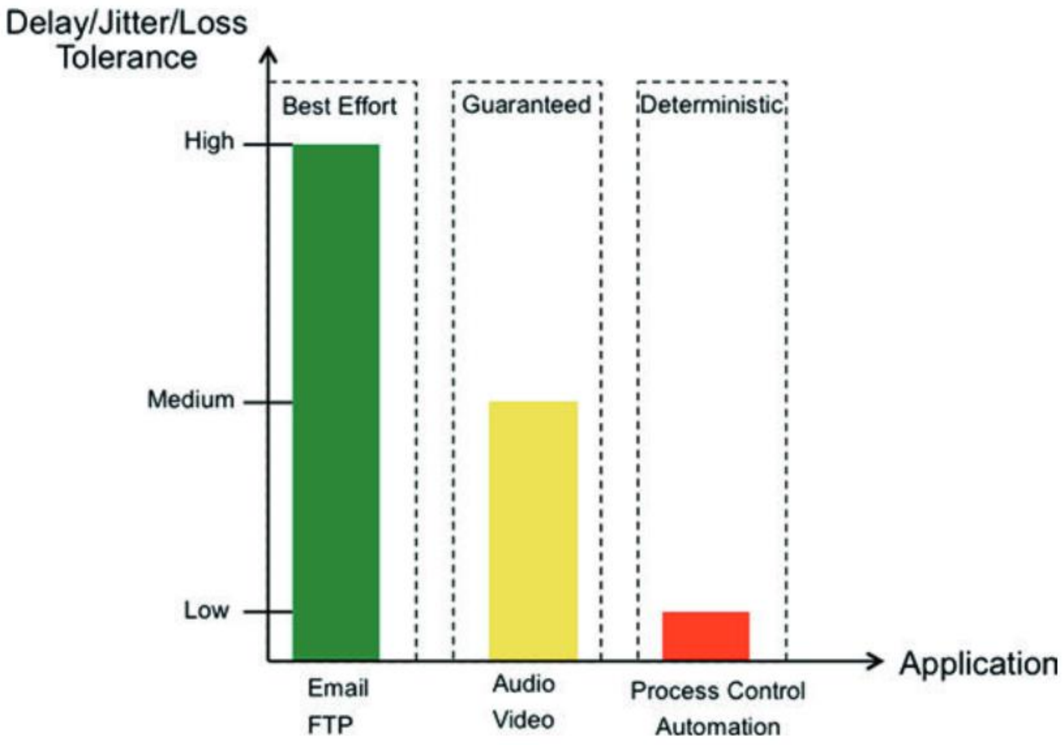
- Systems with control loops involving endpoints communicating over a network can function properly only if the networks connecting those endpoints guarantee determinism

- Imagine what would happen if a network delays a packet carrying a motor angle for a remote surgery!

Challenge 3: Determinism

- What is a *deterministic network* ?

Worst-case communication latency and jitter of messages of interest are decidable based on a reasonable model of the network.



- Enables migration of real-time applications to Internet Protocol based technologies.

- Requires very accurate time synchronization and notion of QoS (Quality-of Service) in the protocol stack

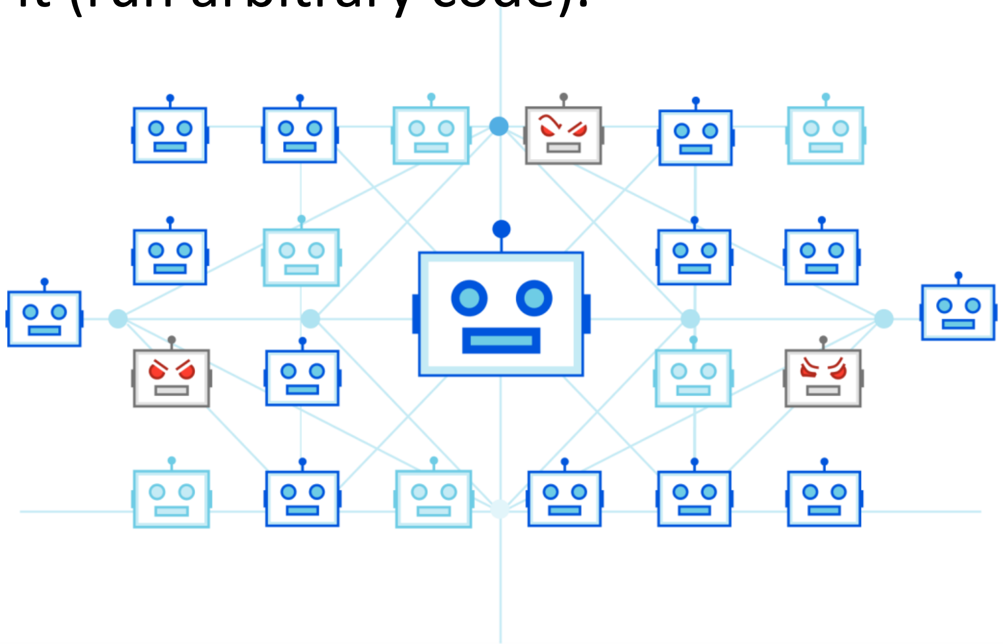
Challenge 4: Security and Privacy

Challenge 4: Security and Privacy

- Case study: MIRAI botnet attack.

- Mirai is a malware that scans the Internet for IoT devices running on the ARC processor.
- These run stripped down version of Linux with default user-name/password combo.
- Mirai is able to log into the device and infect it (run arbitrary code).

- *In 2016: It crippled several high-profile services by launching* *Distributed Denial-of-Service (D-DOS) attacks.*



Challenge 4: Security and Privacy

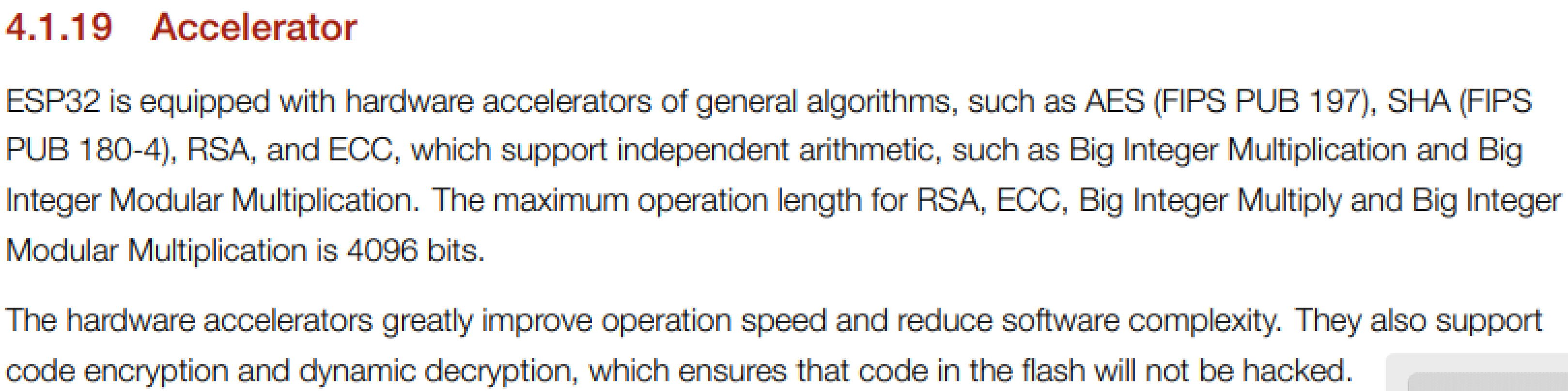
- New lightweight authentication and authorization protocols are required.

- Modern strong encryption/authentication algorithms should be used.
  - DES
  - RSA
  - SHA
  - RNG
  - AES

- However, they should also be capable of running on constrained devices

Challenge 4: Security and Privacy

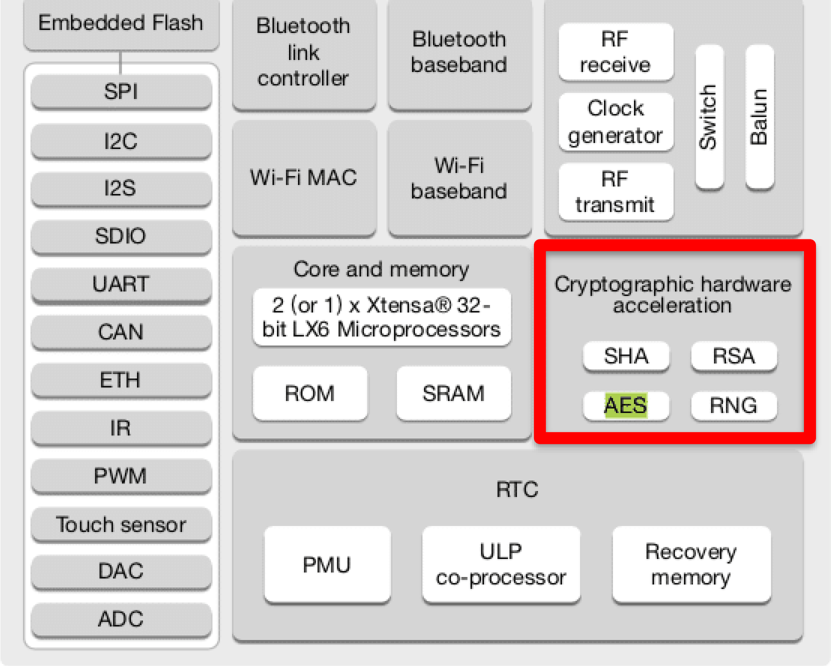
- In ESP32:



4.1.19 Accelerator

ESP32 is equipped with hardware accelerators of general algorithms, such as AES (FIPS PUB 197), SHA (FIPS PUB 180-4), RSA, and ECC, which support independent arithmetic, such as Big Integer Multiplication and Big Integer Modular Multiplication. The maximum operation length for RSA, ECC, Big Integer Multiply and Big Integer Modular Multiplication is 4096 bits.

The hardware accelerators greatly improve operation speed and reduce software complexity. They also support code encryption and dynamic decryption, which ensures that code in the flash will not be hacked.



Challenge 4: Security and Privacy

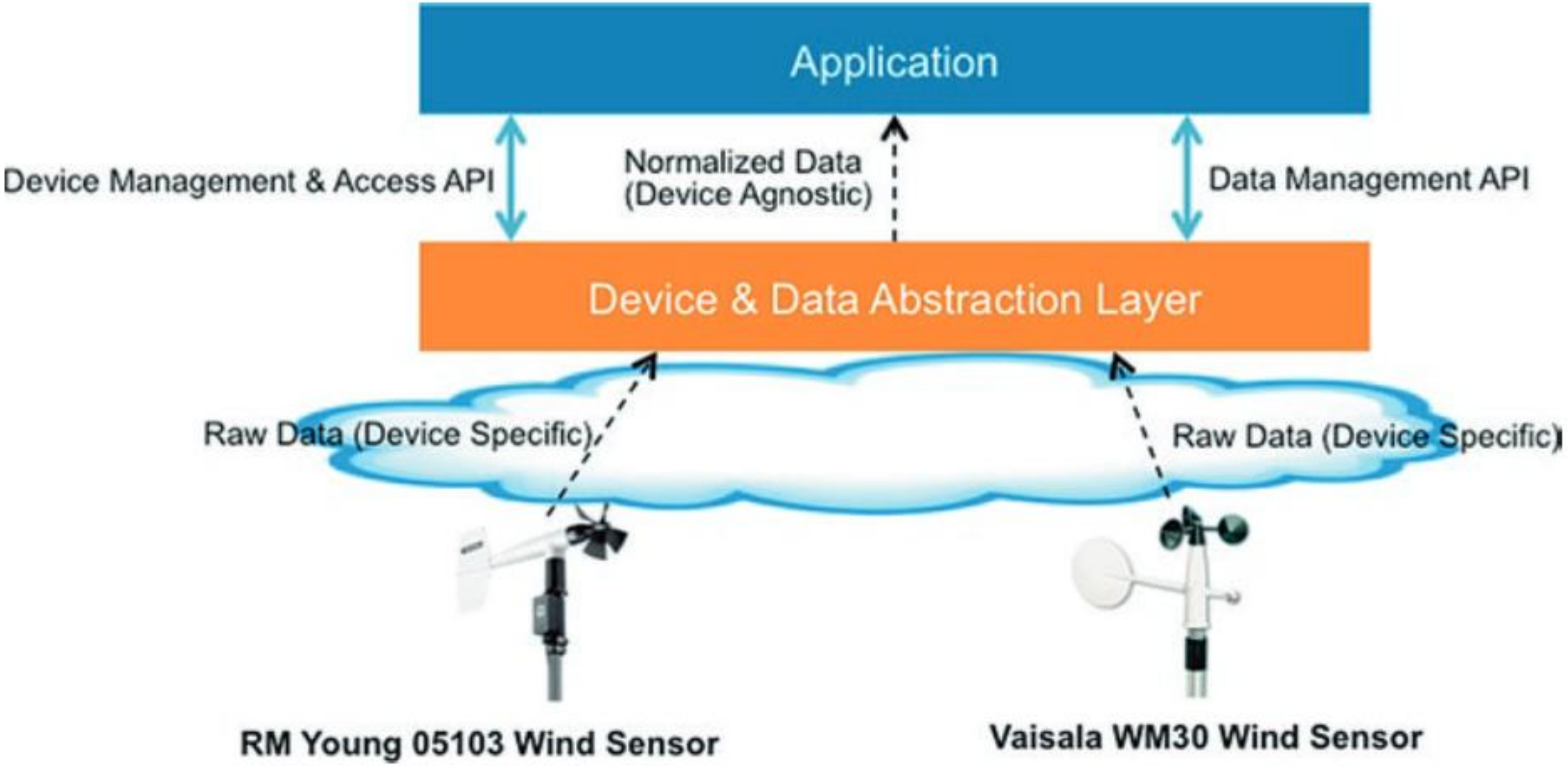
- Privacy is ability of an individual or group to seclude themselves or information about themselves.
- User data is collected for a multitude of purposes such as targeted advertisements, purchase recommendations, and even national security.
- Enormous amounts of information out there!
- Some IoT applications even involve highly sensitive personal information, such as medical records.

INTERNET OF THINGS
APP
INTERCONNECTION
NETWORK
SMART
DATA
AUTOMATION
Is Your IoT Device Safe and Secure?
Managing Security Risks Still a Concern for Many!

Identity Management :

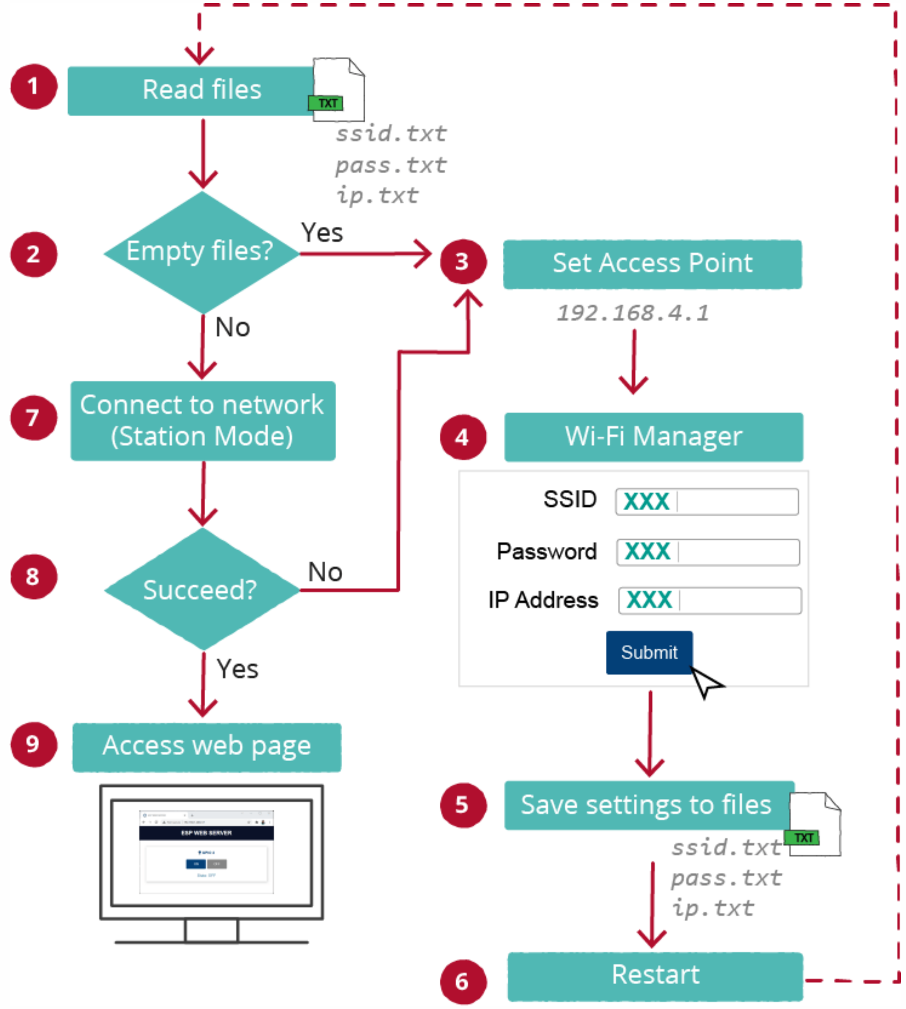
- Decouple device/data from owner’s identity.
- Still provide robust mechanisms for ownership verification and identity authentication.

Challenge 5: Application Interoperability


Application
Device Management & Access API
Normalized Data
(Device Agnostic)
Data Management API
Device & Data Abstraction Layer
Raw Data (Device Specific)
Raw Data (Device Specific)
RM Young 05103 Wind Sensor
Vaisala WM30 Wind Sensor

Demo: Credential Management

- How to “not” hardcode WiFi Credential



1. https://github.com/tzapu/WiFiManager/
2. https://github.com/khoih-prog/ESPAsync_WiFiManager