หน่วยที่ 1

แนะนำ Internet of Things

ผู้ใช้คำว่า “Internet of Things (IoT)” เป็นคนแรก

Kevin Ashton

“I was talking about the supply chain being a ‘Network of Things,’ and the Internet being a ‘Network of Bits,’ and how sensor technology would merge the two together. Then I thought of an ‘Internet of Things,’ and I thought, ‘That’ll do – or maybe even better.’ It had a ring to it. It became the title of the presentation.”

https://blog.avast.com/kevin-ashton-named-the-internet-of-things

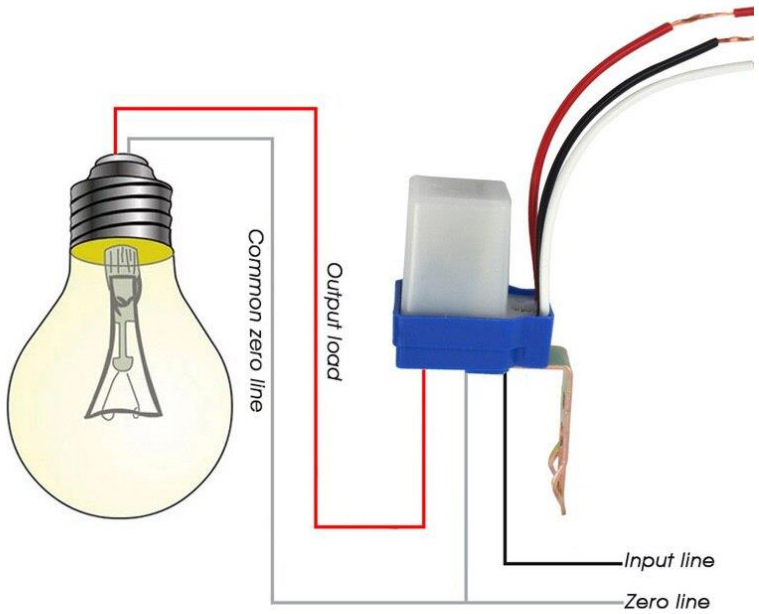
Internet + Things

- Internet = network of network
  - สื่อกลางในการเชื่อมต่อ
  - สถาปัตยกรรม
  - โพรโทคอล
- Things = anything, everything
  - แต่ในความเป็นจริง เมื่อพูดถึง IoT เราจะไม่ได้หมายความรวมถึงเครื่องคอมพิวเตอร์ หรืออะไรที่คล้ายกัน (เช่น เครื่อง smartphone)

Internet of Things

- IoT เชื่อมโลก physical และโลก digital เข้าด้วยกัน
- IoT เชื่อมโลก physical ด้วย sensor, actuator, data converter
- IoT เชื่อมหากันด้วย network รูปแบบต่างๆ
- IoT เก็บข้อมูลจาก sensor ไว้ในโลก digital
- IoT นำข้อมูลจากโลก digital ไปสู่โลก physical ผ่าน actuator

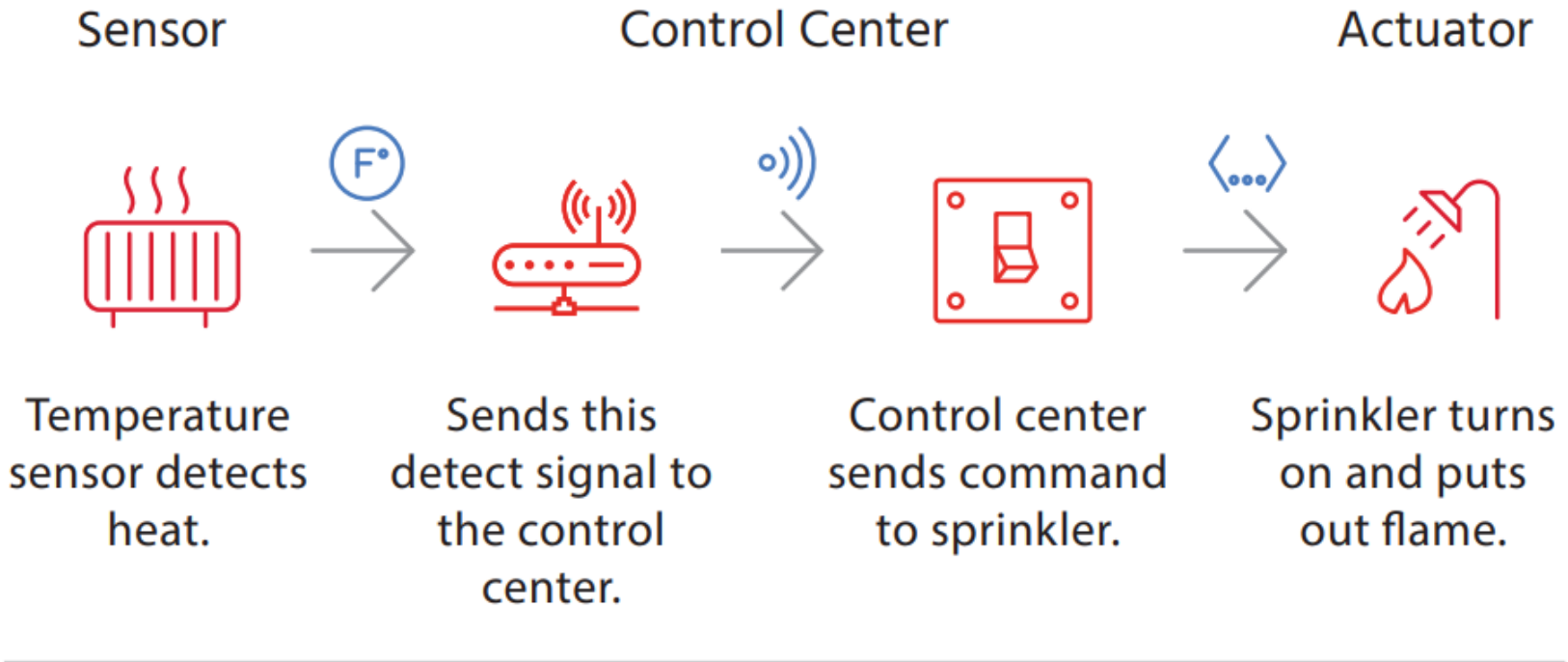
Automatic system



- รับรู้สภาพแวดล้อมด้วย sensor
  - แสงมาก แสงน้อย มีแสง ไม่มีแสง
- ควบคุมระบบโดย actuator
  - รีเลย์ตัดต่อวงจรหลอดไฟส่องสว่าง

IoT

E..., Digital, Internet, Cyber, ...

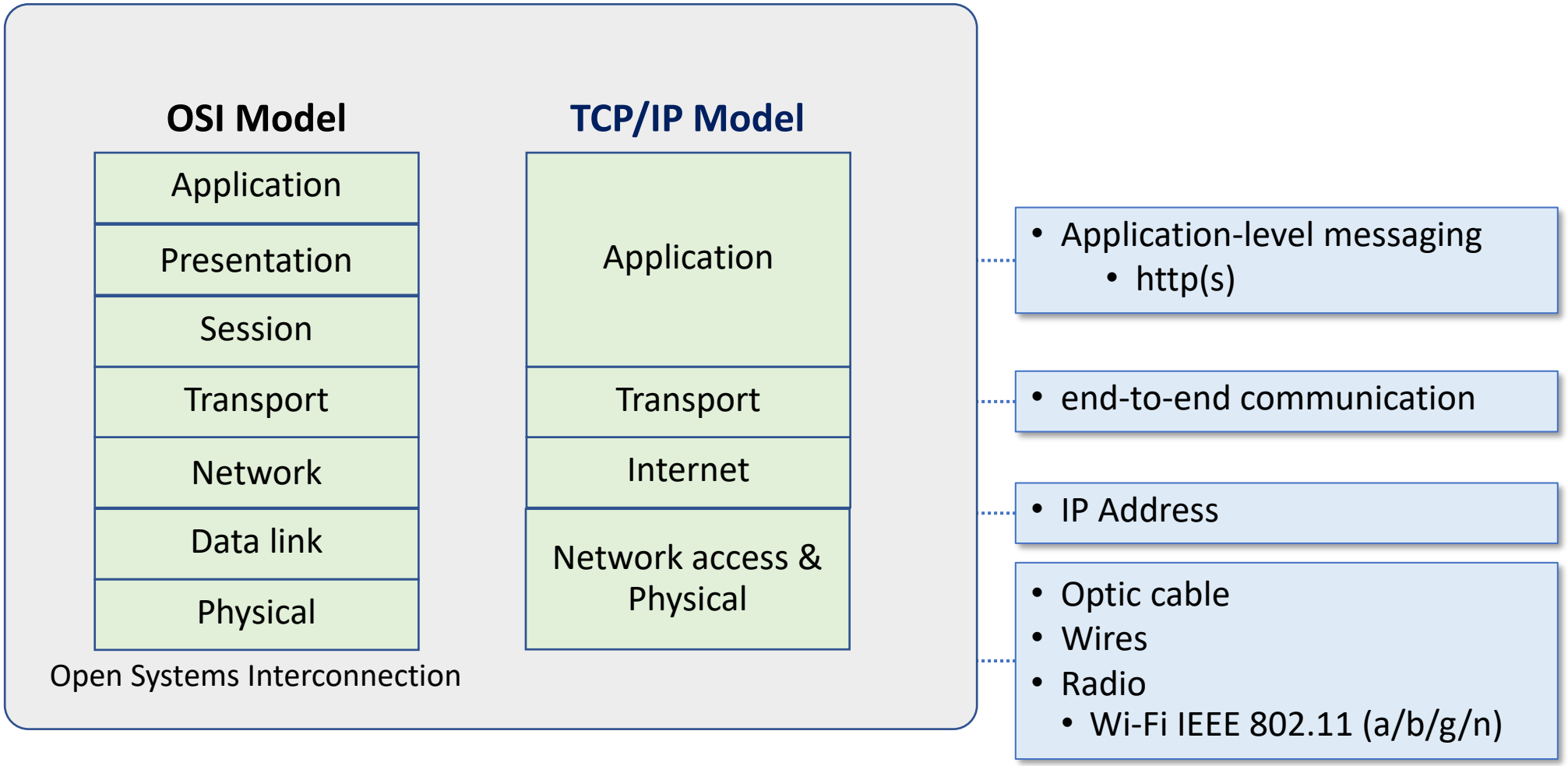


เทคโนโลยีที่เกี่ยวข้องกับการพัฒนา IoT

เทคโนโลยี Internet/Web

- Internet ทำงานบน protocol มาตรฐาน
  - เพื่อความ compatible กับทั้งอุปกรณ์ในอดีตและอนาคต
- Internet มี services มาตรฐาน (ทำงานบน cloud)
- Network จะทำงานบน stack ที่หลากหลาย
- Physical device เดียวกันอาจทำงานได้บนหลาย logical device
  - เช่น network interface card อาจทำงานได้ทั้ง IPv4 และ IPv6

Networking standard & technology

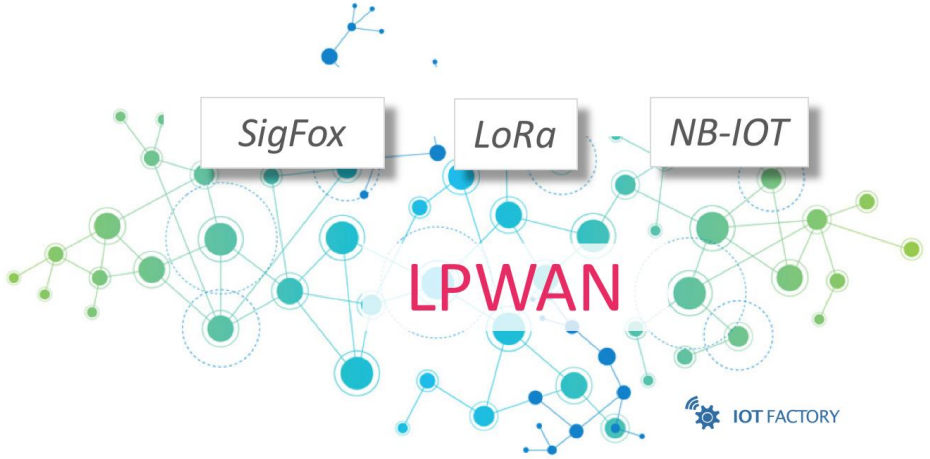


เทคโนโลยีการเข้าถึง network ในระดับชั้น physical

- LPWAN
- Cellular
- Bluetooth Low Energy (BLE)
- ZigBee
- NFC
- RFID
- Wi-Fi
- Ethernet

LPWAN (Low Power Wide Area Network)

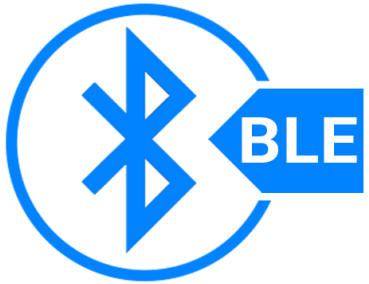
- ออกแบบมาเพื่อใช้กำลังงานต่ำ แต่มีระยะทางในการสื่อสารที่ไกลมาก (low-power, long-range wireless communication)
- เหมาะที่จะใช้กับอุปกรณ์ IoT กำลังงานต่ำ เช่น wireless sensors (network)
- ตัวอย่างเทคโนโลยี LPWAN
  - LoRa (Long-Range physical layer protocol
  - Haystack
  - SigFox
  - LTE-M
  - NB-IoT (Narrow-Band IoT).



Cellular (เครือข่ายโทรศัพท์เคลื่อนที่)

- ออกแบบมาเพื่อใช้งานร่วมกับเครือข่ายโทรศัพท์เคลื่อนที่ มีระยะทางในการสื่อสารครอบคลุม cell site
- LTE-M และ NB-IoT เป็น long range communication ที่ใช้ cellular เป็นสื่อกลาง
- ตัวอย่างเทคโนโลยี cellular
  - 2G (GSM) (อยู่ในสถานะเตรียมเลิกให้บริการ)
  - Code-division multiple access (CDMA) (อยู่ในสถานะเตรียมเลิกให้บริการ)
  - 3G (อยู่ในสถานะเตรียมเลิกให้บริการ)
  - 4G (เป็นระบบหลัก และเตรียมเลิกใช้เมื่อมีระบบ 5G)
  - 5G

Bluetooth Low Energy (BLE)



- ออกแบบมาเพื่อใช้งานในระยะใกล้ (ไม่เกิน 100 เมตร)
- Bandwidth ประมาณ 270 kbps
- มี topology แบบ star คือมีอุปกรณ์ primary หนึ่งตัวเชื่อมต่อกับ secondary หลายตัว
- BLE ทำงานใน 2 layers ของ OSI Model
  - Layer 1 : PHY
  - Layer 2 : MAC
- BLE เหมาะกับระบบที่ส่งข้อมูลไม่มาก และส่งเป็นช่วงๆ (bursts)
- ตัวอย่างเทคโนโลยี BLE
  - หูฟัง
  - อุปกรณ์สวมใส่เพื่อสุขภาพ

ZigBee

- ZigBee ทำงานบนความถี่ย่าน 2.4 GHz
- ออกแบบมาเพื่อใช้งานในระยะไม่เกิน 100 เมตรในที่โล่ง
  - ในอาคารประมาณ 10-20 เมตร
- Bandwidth ประมาณ 250 kbps
- มี topology แบบ mesh (อุปกรณ์ทุกตัวสามารถคุยกันได้ทั้งหมด)
- อุปกรณ์ ZigBee สามารถทำงานได้หลายหน้าที่ เช่นเป็น device ธรรมดา, controller หรือ router
- ZigBee ถูกออกแบบมาใช้กับงาน Home automation

NFC (Near Field Communication)

- NFC ออกแบบมาเพื่อใช้งานในระยะสั้น ประมาณ 4 เซนติเมตร
- ส่วนใหญ่มีลักษณะเป็น tag หรือ card
- นิยมใช้ในระบบ payment, check-in, asset tracking

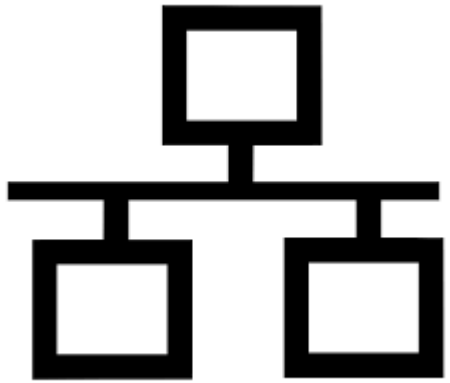
RFID (Radio Frequency Identification)

- RFID tags ทำหน้าที่เก็บข้อมูล (ID)
- ออกแบบมาเพื่อใช้งานในระยะสั้น (ประมาณ 1 เมตร)
- RFID tag มีทั้งแบบ active และ passive
  - Active RFID tag ต้องการแบตเตอรี่ แต่สามารถใช้งานที่ระยะไกลกว่า
  - Passive RFID tag ทำงานได้โดยไม่ต้องใช้แบตเตอรี่
- RFID tag นิยมใช้งานในลักษณะคล้ายกับ NFC

Wi-Fi

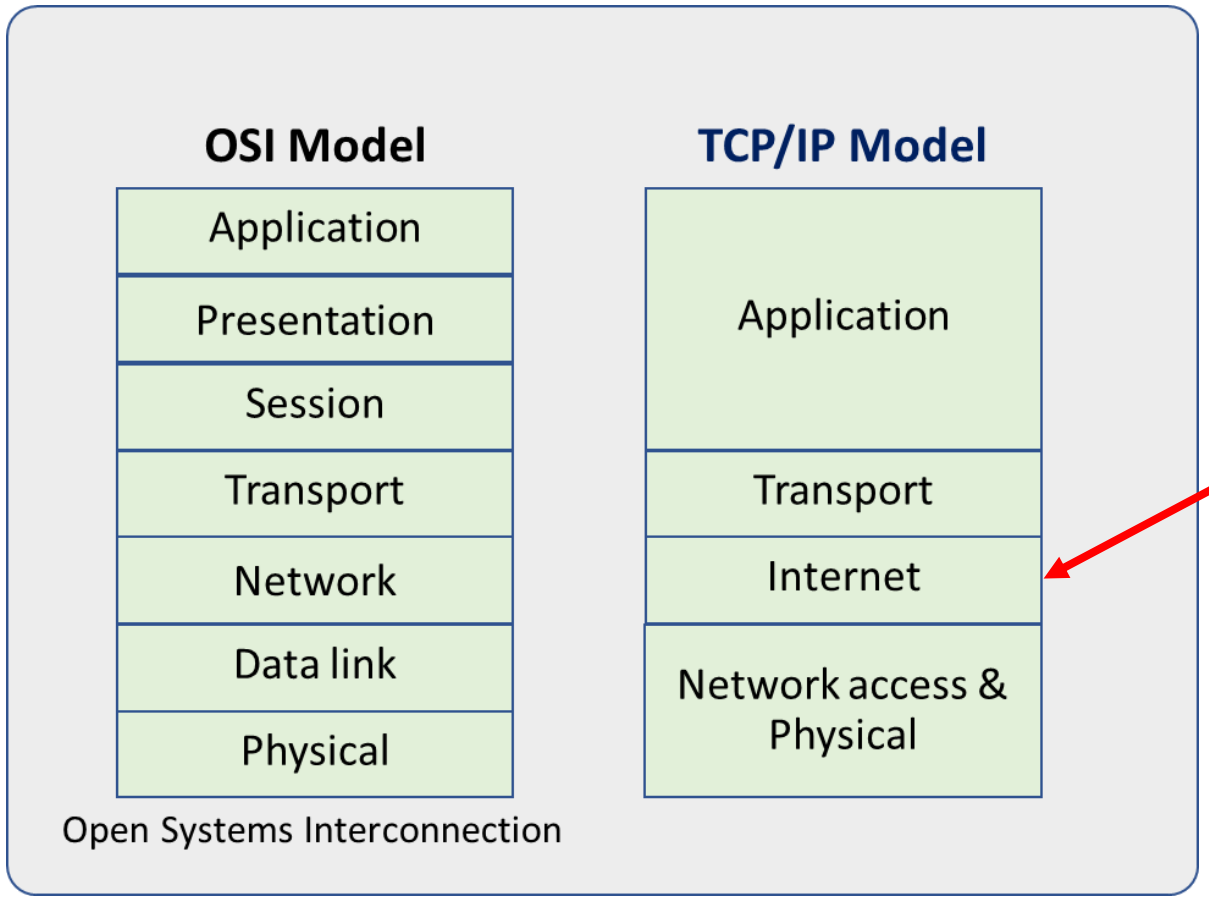
- Wi-Fi เป็นมาตรฐานของ network ที่ใช้คลื่นวิทยุ
- ทำงานบนข้อกำหนด IEEE 802.11a/b/g/n
  - /n จะมีอัตราข้อมูลสูงสุด แต่กินกำลังมากที่สุด
  - ระบบ IoT นิยมใช้ 802.11/b หรือ /g เพื่อประหยัดกำลังงาน
- มีแนวโน้มที่ Wi-Fi จะถูกแทนที่ด้วยเทคโนโลยีที่กินกำลังต่ำกว่า

Ethernet



- เป็นระบบสื่อสารข้อมูลแบบใช้สายที่ได้รับความนิยมสูง
- ทำงานบนข้อกำหนด IEEE 802.3
- เหมาะกับระบบ IoT ที่อยู่กับที่ (Stationary) เช่นภายในอาคาร
- มีคู่แข่งที่สำคัญได้แก่ Power Line Communication (PLC)

Internet Layer IoT Network Technologies



- Internet layer technologies (OSI Layer 3) ทำหน้าที่ในการ identify และ route แพตเกจข้อมูลใน network
- เทคโนโลยีที่ IoT ใช้ใน layer นี้ได้แก่ IPv6, 6LoWPAN, และ RPL

IPv6

- ภายใต้ Internet layer หมายเลขประจำตัวของอุปกรณ์ทุกตัวจะถูกกำหนดด้วย IP addresses
- ในระบบ IoT จะนิยมใช้การอ้าง address แบบ IPv6 มากกว่า IPv4
  - IPv4 จะถูกจำกัด address ไว้ที่ 32-bit (ประมาณ 4,300 ล้านอุปกรณ์)
  - IPv6 ใช้ address ขนาด 128-bit (ประมาณ 340 ล้านล้านล้านล้านอุปกรณ์)
- แต่โดยทั่วไปแล้ว IoT devices มักจะไม่ต้องการใช้ public addresses
  - ส่วนใหญ่จะเข้าถึงโลกภายนอกผ่าน gateway

6LoWPAN

- 6LoWPAN มาจาก IPv6 Low Power Wireless Personal Area Network
- 6LoWPAN เป็นมาตรฐานที่อนุญาตให้ใช้ IPv6 บน 802.15.4 wireless networks.
- 6LoWPAN นิยมใช้กับ
  - wireless sensor networks
  - home automation devices

RPL

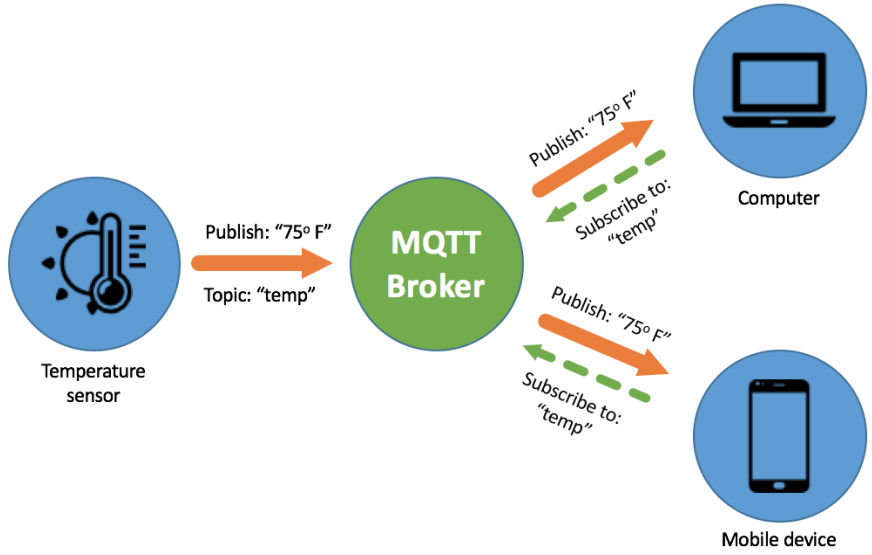
- RPL ออกเสียงว่า “ripple”
- IPv6 ที่ออกแบบมาเพื่องาน Low-Power มักจะมีลักษณะเป็น Lossy Networks
  - ทำงานกับ wireless sensor network ที่ไม่ได้มีการเชื่อมต่ออย่างต่อเนื่อง
  - มีปริมาณ packet loss ที่ไม่สามารถคาดเดาได้
- RPL สามารถคำนวณเส้นทางที่เหมาะสมสำหรับการสื่อสารข้อมูล โดยสร้างกราฟขึ้นจาก node ใน network แบบ dynamic
  - โดยคำนึงถึงการใช้พลังงานน้อยที่สุด (minimize energy) และเสียเวลาในการสื่อสารน้อยที่สุด (minimize latency time)

เทคโนโลยีในระดับ Application Layer

- โดยปกติ แอปพลิเคชันที่ใช้งานทั่วไปบนอินเทอร์เน็ตคือ HTTP และ HTTPS ซึ่งใน IoT ก็เป็นความจริงเช่นกัน
  - แต่จะใช้อินเทอร์เฟซ RESTful HTTP และ HTTPS ซึ่งผ่านการปรับแต่งแล้ว (CoAP)
  - มีลักษณะเป็น HTTP ขนาดย่อส่วนที่ใช้ร่วมกับ 6LoWPAN บน UDP
- นอกจากนี้ ยังมีโปรโตคอลที่นิยมใช้ ได้แก่
  - MQTT
  - AMQP
  - XMPP

MQTT (Message Queue Telemetry Transport)

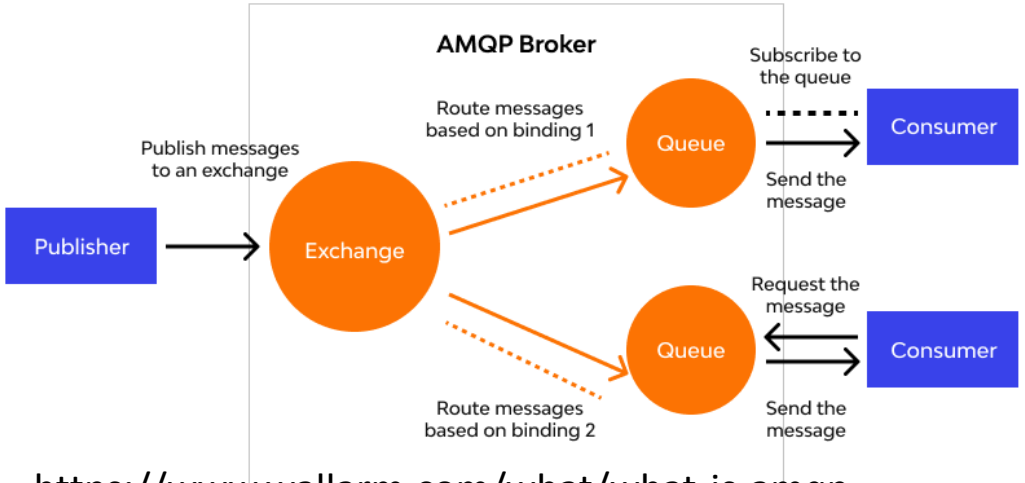
- MQTT เป็นโพรโทคอลแบบ publish/subscribe-based messaging
- ถูกออกแบบมาให้ใช้กับระบบที่ใช้ bandwidth ต่ำและไม่เน้นเสถียรภาพในการเชื่อมต่อ



https://miro.medium.com/max/1400/1*PO5_87H8ZHRGWQpeOAFXMA.png

AMQP (Advanced Message Queuing Protocol)

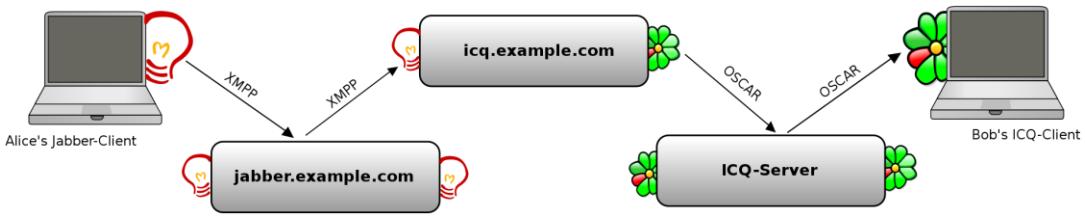
- AMQP เป็นโพรโทคอลแบบ open standard messaging
- เป็นโพรโทคอลที่ใช้กับ message-oriented middleware.
- AMQP ได้รับการพัฒนาโดย RabbitMQ



https://www.wallarm.com/what/what-is-amqp

XMPP (Extensible Messaging and Presence Protocol)

- XMPP ถูกออกแบบมาเพื่อใช้กับระบบสื่อสารแบบ real-time สำหรับมนุษย์ (real-time human-to-human communication)
- แต่แล้วโพรโทคอลนี้ก็ถูกปรับมาใช้สำหรับการสื่อสารระหว่างเครื่อง (machine-to-machine (M2M) communication)
- วัตถุประสงค์หลักคือเป็นส่วนทำงานและส่งผ่าน XML data
- XMPP นิยมใช้กับเครื่องใช้อัจฉริยะ



https://en.wikipedia.org/wiki/XMPP#/media/File:Wie_ein_Jabber-Transport_funktioniert.svg

ความท้าทายในการสร้างระบบ IoT

ต้องมี Internet hardware/protocols ที่หลากหลาย

- ระยะทางในการรับส่งข้อมูล (range)
- Bandwidth
- กำลังงานที่ใช้ (Power usage)
- ลักษณะการเชื่อมต่อ เช่นเชื่อมต่อตลอดเวลาหรือ ad hoc
- การทำงานร่วมกับระบบอื่น ๆ (interoperability)
- ความปลอดภัย (security)

ระยะทางในการรับส่งข้อมูล (range)

- ระยะทางในการรับส่งข้อมูล (range) คือระยะห่างระหว่างอุปกรณ์ IoT oy[เป็นปัจจัยสำคัญในการเลือก (ออกแบบ) ระบบ IoT โดยเราต้องเลือกให้เหมาะสมกับ Application ที่ต้องการ
- ขนาดของเครือข่าย IoT แบ่งตามระยะห่างระหว่างอุปกรณ์ได้ดังนี้
  - PAN (Personal Area Network)
  - LAN (Local Area Network)
  - MAN (Metropolitan Area Network)
  - WAN (Wide Area Network)

PAN (Personal Area Network)

- PAN เป็นเครือข่ายที่มีระยะทางระหว่างอุปกรณ์สั้นที่สุด มีระยะไม่กี่เซนติเมตรถึงไม่กี่เมตร
  - เช่น อุปกรณ์ติดตามข้อมูลสุขภาพ (wearable fitness tracker device)
  - เชื่อมต่อกับ smartphone ผ่าน BLE

LAN (Local Area Network)

- LAN เป็นเครือข่ายที่มีระยะห่างระหว่างอุปกรณ์ในช่วงสั้นถึงช่วงกลาง
- สื่อสารข้อมูลได้ในระยะไกลหลายร้อยเมตร
  - เช่น ระบบอัตโนมัติภายในบ้านหรือเซ็นเซอร์ที่ติดตั้งภายในโรงงานผลิต
  - สื่อสารผ่านสาย Ethernet หรือ Wi-Fi
  - อุปกรณ์ที่ทำหน้าที่เกตเวย์มักจะติดตั้งอยู่ภายในอาคารเดียวกัน

MAN (Metropolitan Area Network)

- MAN จัดเป็นเครือข่ายการสื่อสารระยะไกล (Long range)
- อาณาเขตของ MAN ครอบคลุมระดับเมือง (city-wide)
- มีระยะทางได้มากหลายกิโลเมตร
  - เช่น เซ็นเซอร์จอดรถอัจฉริยะติดตั้งทั่วเมือง ที่เชื่อมต่อในโทโพโลยีเครือข่ายแบบเมช

WAN (Wide Area Network)

- WAN จัดเป็นเครือข่ายการสื่อสารระยะไกล (Long range)
- อาณาเขตของ WAN มักจะวัดกันในหน่วยกิโลเมตร
- มีระยะทางได้มากหลายกิโลเมตร
  - เช่น เซนเซอร์ทางการเกษตร ที่ติดตั้งในฟาร์มขนาดใหญ่ หรือระบบเครือข่ายพยากรณ์อากาศที่ครอบคลุทระดับภูมิภาคของประเทศ

Bandwidth

- Bandwidth วัดจากจำนวนข้อมูลที่สามารถส่งได้ต่อหน่วยเวลา
- Bandwidth เป็นตัวกำหนดอัตราข้อมูลที่สามารถรวบรวมข้อมูลจากอุปกรณ์ IoT และส่งไปยังปลายทาง
- ปัจจัยที่ส่งผลกระทบต่อ Bandwidth :
  - ปริมาณข้อมูลที่แต่ละอุปกรณ์ IoT รวบรวมมาได้และส่งเข้าสู่เครือข่าย
  - จำนวนอุปกรณ์ IoT ที่ใช้งานต่อระบบ
  - รูปแบบการส่งข้อมูลในระบบ (ส่งด้วยอัตราคงที่ ส่งเป็นช่วงๆ หรือส่งตามเหตุการณ์ที่สนใจ)

Bandwidth

- การเลือกระบบที่มี bandwidth ที่ไม่เหมาะสม อาจจะไม่ก่อให้เกิดปัญหาร้ายแรง แต่ทำให้ต้องใช้ความพยายามเพิ่มขึ้น
  - ถ้าข้อมูลจากอุปกรณ์ IoT มีขนาดเล็กกว่า packet ต้องเติมด้วยข้อมูลบางอย่าง (padded with empty data)
  - ถ้าข้อมูลจากอุปกรณ์ IoT มีขนาดโตกว่า packet ต้องแบ่งออกเป็นหลายส่วน แล้วทยอยส่งในระบบ
- Bandwidth ของฝั่งรับและส่งอาจจะไม่เท่ากัน
  - เช่น download 10MBps, Upload 2MBps

*** ในกรณีที่ข้อมูลไม่ match กับ bandwidth การจัดการทุกอย่างให้เหมาะสม จะใช้ทรัพยากรทั้งหน่วยความจำและการประมวลผลที่เพิ่มขึ้น

กำลังงานที่ใช้ (Power usage)

- การส่งข้อมูลจากอุปกรณ์ IoT ต้องใช้พลังงาน
  - การส่งข้อมูลในระยะไกลต้องการพลังงานมากกว่าระยะสั้น
- ในบางกรณี เราอาจต้องใช้แบตเตอรี่ โซลาร์เซลล์ หรือตัวเก็บประจุขนาดใหญ่ (Super capacitor)
- การใช้พลังงานอย่างประหยัด
  - ช่วยให้ระบบมีอายุการใช้งานที่นานขึ้น
  - มีความน่าเชื่อถือมากขึ้น
  - ลดต้นทุนการดำเนินงานอีกด้วย
- เทคนิคการลดใช้พลังงาน
  - ทำให้อุปกรณ์เข้าสู่โหมดสลีปเมื่อไม่ได้ใช้งาน
  - เลือกเครือข่ายที่เหมาะสม
  - เลือก Bandwidth ที่เหมาะสม

ลักษณะการเชื่อมต่อ

- อุปกรณ์ IoT อาจจะไม่ได้เชื่อมต่อกับเครือข่ายตลอดเวลา
  - ในบางกรณี อุปกรณ์ได้รับการออกแบบมาเพื่อเชื่อมต่อเป็นห้วง ๆ
  - บางครั้งเครือข่ายที่ไม่มีเสถียรภาพ อาจทำให้อุปกรณ์หลุดออกมา
- ปัญหาการเชื่อมต่ออาจจะมีสาเหตุมาจาก
  - คุณภาพของบริการ
  - สัญญาณรบกวนและการรบกวน
  - การแบ่งช่องสัญญาณโดยใช้คลื่นความถี่ที่ใช้ร่วมกัน
- การออกแบบระบบอาจจะต้องออกแบบให้รองรับการเชื่อมต่อได้ในหลาย ๆ รูปแบบ

การทำงานร่วมกับระบบอื่น ๆ

- อุปกรณ์ IoT จำเป็นทำงานร่วมกับอุปกรณ์ เครื่องมือ ระบบ และเทคโนโลยีอื่น ๆ ที่มีอยู่หรือเกิดขึ้นในอนาคต
- ความท้าทายอยู่ที่เราต้องสามารถทำให้อุปกรณ์ IoT ทำงานร่วมกันได้
  - ใช้โพรโทคอลมาตรฐาน (ถ้าโพรโทคอลที่มีอยู่เดิมใช่ได้ดี ก็ใช้ต่อไป)
  - หลีกเลี่ยงการออกแบบด้วยมาตรฐานที่หลากหลาย
  - แต่บางครั้งกระบวนการสร้างมาตรฐานก็ต้องดิ้นรนเพื่อให้ทันนวัตกรรมและการเปลี่ยนแปลง ทำให้ผู้สร้างมาตรฐานต้องเขียนและเผยแพร่ตามกรอบเวลา ทั้ง ๆ ที่มาตรฐานยังคงมีการเปลี่ยนแปลง
- พิจารณาระบบนิเวศโดยรอบว่าควรกำหนดระบบ IoT ของเราไปในทิศทางใด

ความปลอดภัย (Security)

- ความปลอดภัย (Security) เป็นสิ่งสำคัญ
  - ควรเลือกใช้เทคโนโลยีเครือข่ายที่สามารถรักษาความปลอดภัยแบบ end-to-end
- ตัวอย่างความปลอดภัย
  - การตรวจสอบสิทธิ์ (Authentication)
  - การเข้ารหัส (Encryption)
  - การป้องกันการละเมิดด้วยการเปิดพอร์ต (Port protection)

การตรวจสอบสิทธิ์

- การตรวจสอบสิทธิ์ ใช้โปรโตคอลที่ปลอดภัยเพื่อรองรับการรับรองความถูกต้องสำหรับ
  - อุปกรณ์ (Devices)
  - เกตเวย์ (Gateways)
  - ผู้ใช้ (Users)
  - บริการ (Services)
  - และแอพพลิเคชั่น (Applications)
- พิจารณาใช้มาตรฐาน X.509 สำหรับการรับรองความถูกต้องของอุปกรณ์

การเข้ารหัส

- ถ้าระบบ IoT ของเราใช้ Wi-Fi
  - ให้ใช้ Wireless Protected Access 2 (WPA2) สำหรับเครือข่ายไร้สาย
  - หรือใช้ไพรเวท Pre-Shared Key (PPSK)
- เพื่อให้มั่นใจว่าในความเป็นส่วนตัวและความสมบูรณ์ของข้อมูลสำหรับการสื่อสารระหว่างแอปพลิเคชัน
  - ทำให้แน่ใจว่าได้ใช้ TLS
  - หรือใช้ Datagram Transport-Layer Security (DTLS) ซึ่งอิงตาม TLS แต่ได้รับการดัดแปลงเพื่อใช้กับการเชื่อมต่อที่ไม่น่าเชื่อถือ (ซึ่งทำงานผ่าน UDP)

Port protection

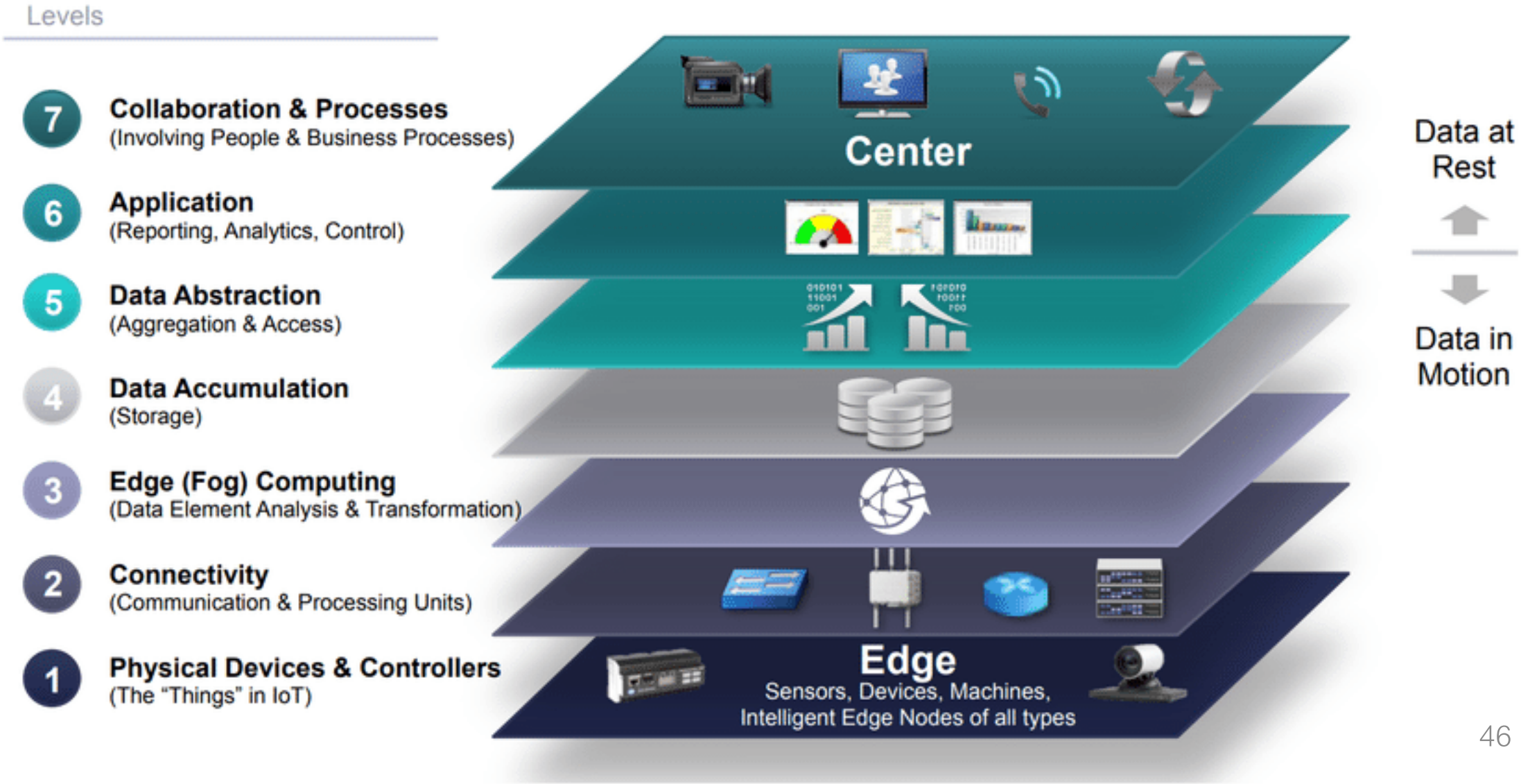
- การป้องกันพอร์ตช่วยให้เรามั่นใจได้ว่า เฉพาะพอร์ตที่จำเป็นสำหรับการสื่อสารกับเกตเวย์หรือแอปพลิเคชันหรือ upstream เท่านั้น ที่สามารถเปิดให้ภายนอกติดต่อเข้ามาได้
- พอร์ตอื่นๆ ที่เหลือทั้งหมดในอุปกรณ์ควรปิดใช้งานหรือป้องกันโดย Firewall
- พอร์ตของอุปกรณ์ของเราอาจถูกเปิดเผยจากช่องโหว่ของ Universal Plug and Play (UPnP) ดังนั้นควรปิดการใช้งาน UPnP บนเราเตอร์ด้วย

The IoT World Forum (IoTWF) Standardized Architecture

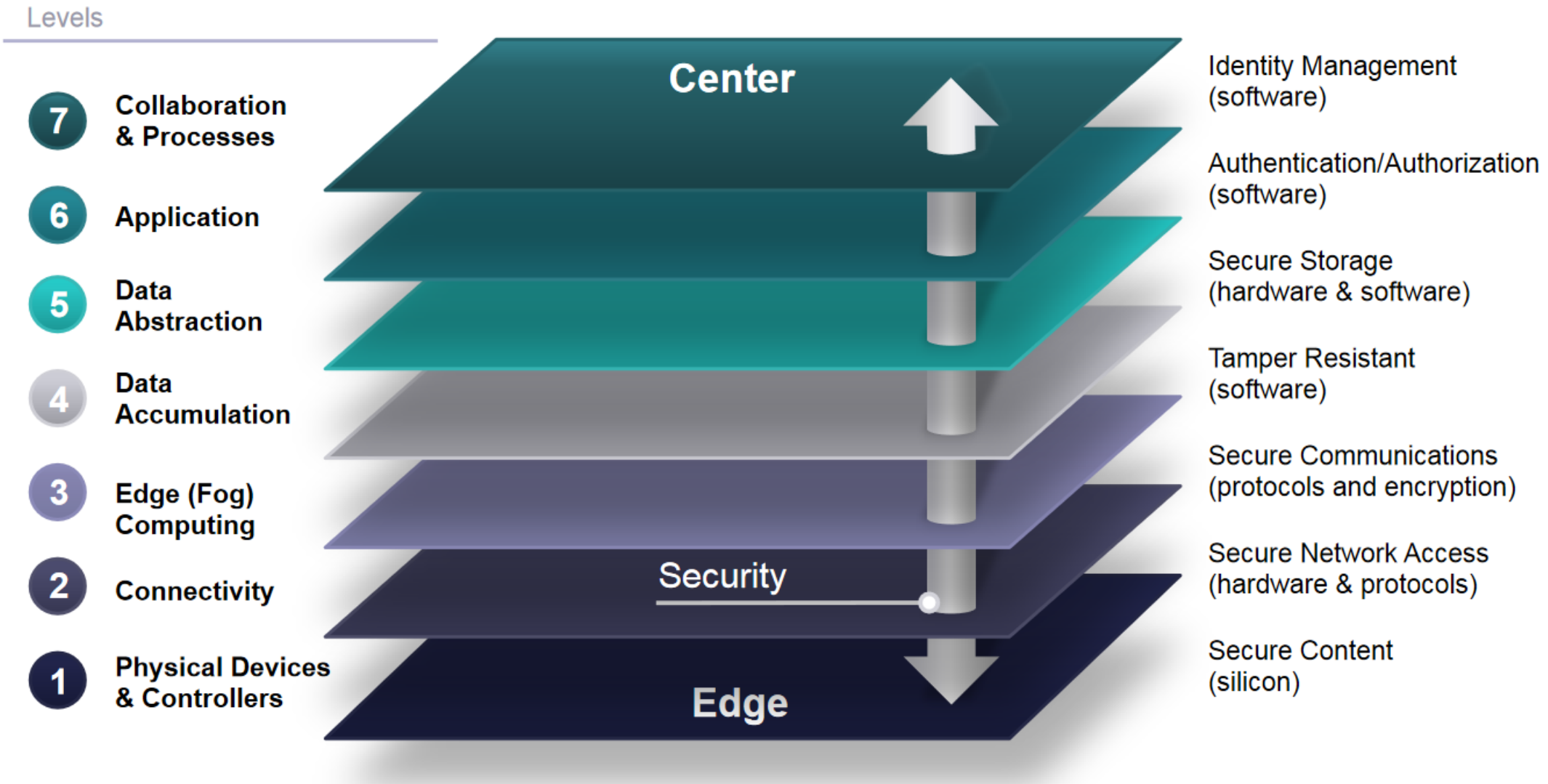
IoTWF Standardized Architecture

- ในปี 2014 คณะกรรมการสถาปัตยกรรม IoTWF (นำโดย Cisco, IBM, Rockwell Automation และอื่น ๆ) เผยแพร่แบบจำลองสถาปัตยกรรม IoT เจ็ดชั้น
- โมเดล อื่น ๆ ของ IoT ที่มีอยู่ ก็ได้รับการทำให้เรียบง่ายและชัดเจนโดย IoTWF เช่น
  - edge computing
  - การจัดเก็บและการเข้าถึงข้อมูล
- สถาปัตยกรรม IoT ช่วยให้มองภาพ IoT จากมุมมองทางเทคนิคที่กระชับขึ้น
- แต่ละชั้นแบ่งออกเป็นฟังก์ชันเฉพาะ
- มีการรักษาความปลอดภัยครอบคลุมทุกชั้นของทั้งโมเดล

Cisco's IoT security reference model



Internet of Things Reference Model: Security



https://devopedia.org/images/article/344/6695.1624617652.png

IoT Reference Model ช่วยอะไรแก่เราบ้าง

- แบ่งระบบ IoT ออกเป็นส่วนย่อย ๆ ระดับย่อย ๆ สามารถแก้ปัญหาได้ง่ายขึ้น
- ระบุเทคโนโลยีต่าง ๆ ของอุปกรณ์ที่ใช้ในแต่ละชั้นและความสัมพันธ์ซึ่งกันและกัน
- กำหนดระบบที่ผู้ขายแต่ละรายสามารถจัดหาชิ้นส่วนต่าง ๆ ให้เราได้
- มีกระบวนการกำหนดอินเทอร์เฟซ ที่นำไปสู่การทำงานร่วมกันของอุปกรณ์ต่าง ๆ
- กำหนดรูปแบบการรักษาความปลอดภัยในแต่ละระดับ รวมถึงรูปแบบที่บังคับใช้ในการสื่อสารข้อมูลระหว่างระดับ

Layer 1: Physical Devices and Controllers Layer

- ชั้นที่ 1 ของแบบจำลองอ้างอิง IoT คือ
  - Physical devices
  - Controller
- ชั้นนี้เป็นที่ตั้งของ "สิ่งของ: Thing" ใน Internet of Things รวมถึงอุปกรณ์ปลายทางต่างๆ
  - sensor และ actuator ที่ส่งและรับข้อมูล
- ขนาดของ “สิ่งของ” เหล่านี้มีตั้งแต่
  - เซนเซอร์ขนาดเล็กระดับมิลลิเมตรถึงนาเมตร
  - เครื่องจักรขนาดยักษ์ในโรงงาน เครื่องบิน รถไฟฟ้าความเร็วสูง ดาวเทียม สถานีอวกาศ
- หน้าที่หลักคือ การสร้างข้อมูล สามารถสอบถาม และ/หรือควบคุมผ่านเครือข่ายได้

Layer 2: Connectivity Layer

- ชั้นที่ 2 ของแบบจำลอง จะโฟกัสอยู่ที่การเชื่อมต่อ
- หน้าที่ของชั้นนี้คือ
  - การส่งข้อมูลที่เชื่อถือได้และทันเวลา (สำคัญที่สุด)
  - การรับ-ส่งข้อมูลระหว่างอุปกรณ์ในชั้นที่ 1
  - การรับ-ส่งข้อมูลระหว่างเครือข่ายต่างชนิดในชั้นที่ 2
  - การรับ-ส่งข้อมูลระหว่างเครือข่ายกับการประมวลผลข้อมูลที่เกิดขึ้นในชั้นที่ 3 (edge computing)
- ชั้นการเชื่อมต่อนี้ ครอบคลุมองค์ประกอบเครือข่ายทั้งหมดของ IoT

② **Connectivity**
(Communication and Processing Units)

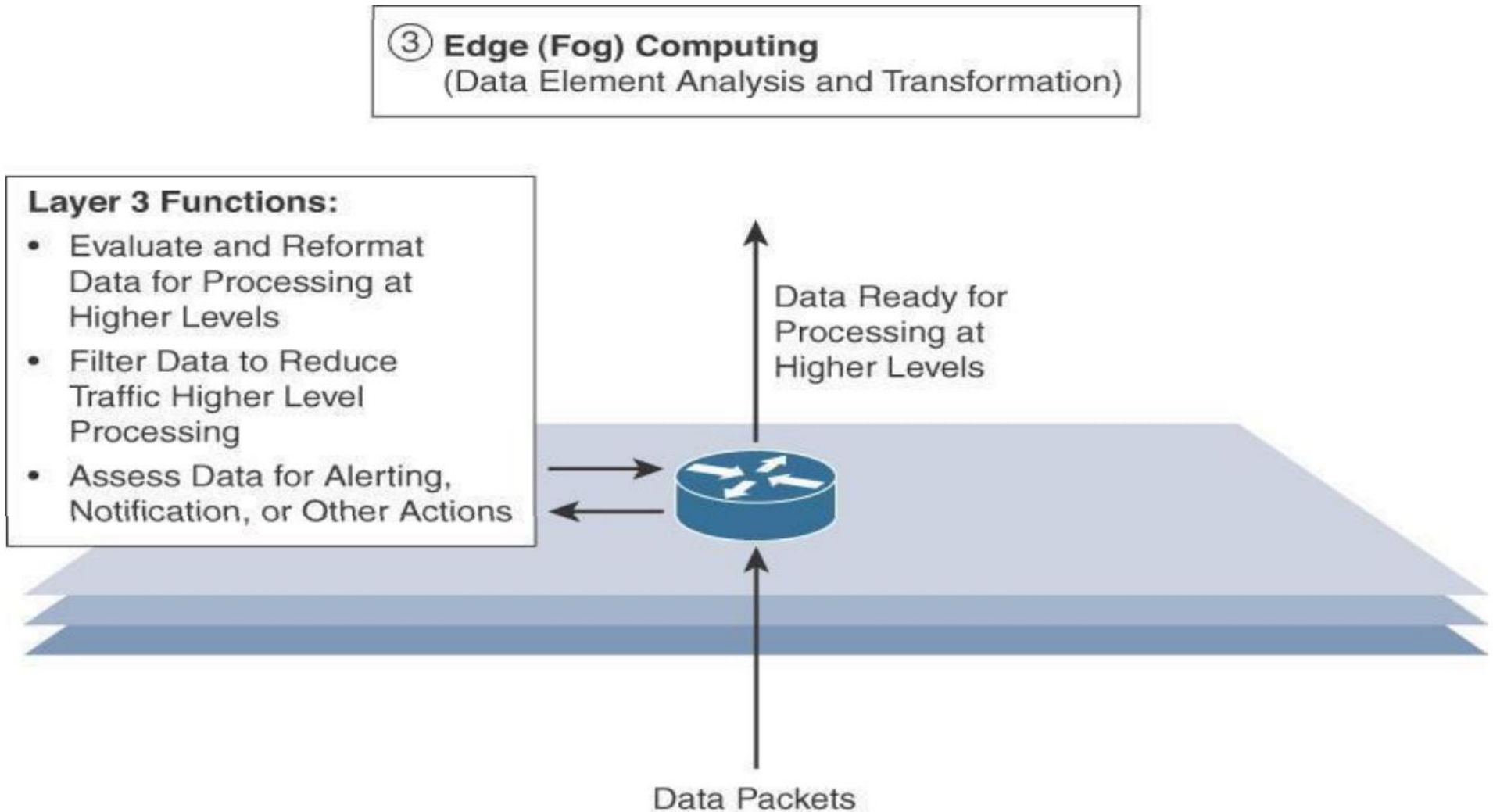
Layer 2 Functions:

- Communications Between Layer 1 Devices
- Reliable Delivery of Information Across the Network
- Switching and Routing
- Translation Between Protocols
- Network Level Security

IoT Reference Model Connectivity Layer Functions

Layer 3: Edge Computing Layer

- ชั้นที่ 3 เป็นที่ตั้งของส่วนประมวลผล ขนาดย่อม ดังนั้นจึงถูกเรียกว่า fog computing (หน่วยประมวลผลหมอก) ซึ่งเล็กกว่า cloud (เมฆ)
- บทบาทสำคัญคือการการลดขนาดข้อมูลและแปลงกระแสข้อมูลเครือข่ายให้เป็นข้อมูลที่พร้อมสำหรับการจัดเก็บและประมวลผลโดยชั้นที่สูงขึ้น
- ชั้นที่สามนี้ จัดเป็นส่วนประมวลผลข้อมูลที่ใกล้กับอุปกรณ์ที่ปลายทางของเครือข่ายมากที่สุด (จึงได้ชื่อว่า “edge computing layer”)



IoT Reference Model Layer 3 Functions

Upper Layers: Layers 4–7

- ชั้นบนของแบบจำลอง มีหน้าที่จัดการประมวลผลข้อมูล IoT ที่สร้างขึ้นโดยชั้นล่าง
  - **Layer 4: Data Accumulation Layer**
  - **Layer 5: Data Abstraction Layer**
  - **Layer 6: Application Layer**
  - **Layer 7: Collaboration Layer**

Layer 4: Data Accumulation

- ทำหน้าที่ตรวจจับและเก็บข้อมูลที่จำเป็นสำหรับ Application
- แปลง event-based data เป็น query-based processing

Layer 5: Data Abstraction Layer

- หลอมรวมข้อมูลหลาย format ให้เป็นข้อมูลที่ใช้งานได้และสอดคล้องกัน
- ตรวจสอบความสมบูรณ์ของ dataset

Layer 6: Application Layer

- แปลความหมายของข้อมูล โดยใช้ software application
- Application สามารถ monitor, control และทำรายงานบนข้อมูลที่วิเคราะห์แล้ว

Layer 7: Collaboration and processes Layer

- ใช้งานและแจกจ่าย application information
- ในการแจกจ่าย IoT information อาจจะต้องมีการประมวลผลเพิ่มเติมอีกหลายขั้นตอน
- ในชั้นที่ 7 นี้อาจจะมีกระบวนการเพิ่มเติม เพื่อให้ได้ประโยชน์สูงสุดจากระบบ IoT ระบบนี้

หน่วยการเรียนรู้ถัดไป

- สถาปัตยกรรม IoT
- IoT Devices
  - Microcontroller
  - Sensor
  - Actuator

คำถาม