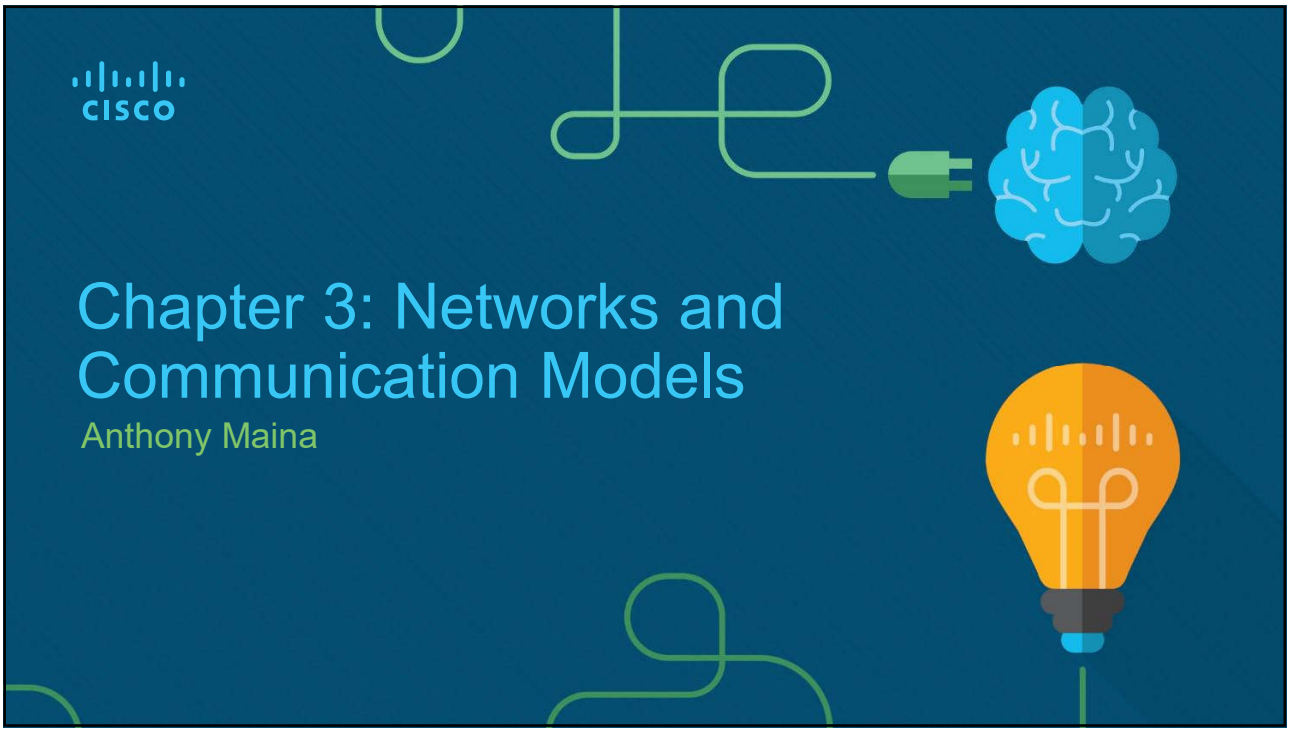


Chapter 3 - Sections & Objectives

- 3.1 What is a network in the IoT era?
  - Describe the basics of a computer network
  - Explain the differences between a traditional network and a network in the IoT era
  - Explain the layered IoT reference model
- 3.2 What are the communication models used in the Internet of Things
  - Explain the different models devices will use to connect to the Internet of Things.

3.1 Networks and layered model

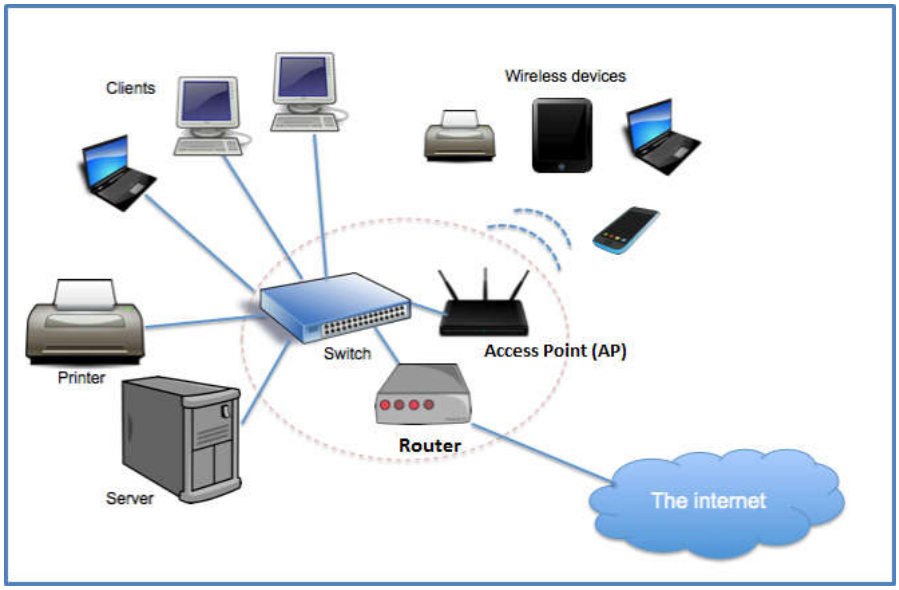
Introduction

- Fifty billion things provide trillions of gigabytes of data.
- How can they work together to enhance our **decision-making** and **interactions** to improve our lives and our businesses?
- Enabling these connections are the networks that we use daily. These networks provide the **foundation for the Internet** and, ultimately, the **IoT**.

Networks

- Simple networks in homes enable **sharing of resources**, such as printers, documents, pictures, and music between a few local computers.
- In businesses and large organizations, networks can provide products and services to customers through their connection to the Internet. Networks can also be used on an even broader scale to provide **consolidation**, **storage**, and **access to information** on network servers. Networks allow for **email**, **instant messaging**, and **collaboration** among employees.
- The Internet is the largest network in existence. In fact, the term Internet means a "***network of networks***." The Internet is literally a collection of interconnected private and public networks. Businesses, small office networks, and even home networks usually provide a shared connection to the Internet.

Network



Network components

- **Devices** and **media** are the physical elements, or hardware, of the network. Hardware is often the visible components of the network platform such as a laptop, PC, switch, router, wireless access point, or the cabling used to connect the devices. Occasionally, some components may not be so visible. In the case of wireless media, messages are transmitted through the air using invisible radio frequency or infrared waves.
- Network components are used to provide **services** and processes. These are the communication programs, called software, that run on the networked devices. A **network service** provides information in response to a request.
- Services include many of the common network applications people use every day, like **email hosting services** and **web hosting services**. Processes provide the functionality that directs and moves the messages through the network.

Network components – end devices

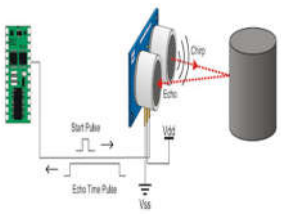
- These devices form the **interface between users** and the underlying **communication network**.
- Some examples of **end devices** are:
- *Computers (workstations, laptops, file servers, and web servers)*
- *Network printers*
- *VoIP phones*
- *TelePresence endpoints*
- *Security cameras*
- *Mobile handheld devices (smartphones, tablets, PDAs, and wireless debit/credit card readers and barcode scanners)*
- *Sensors such as thermometers, weight scales, and other devices that will be connected to the IoT*

Network components – end devices (types of sensors)

- ***Temperature Sensors*** – they measure the amount of heat energy in a source, allowing them to detect temperature changes and convert these changes to data. Machinery used in manufacturing often requires environmental and device temperatures to be at specific levels. Similarly, within agriculture, soil temperature is a key factor for crop growth.
- ***Humidity Sensors –*** they measure the amount of water vapor in the atmosphere of air or other gases. Humidity sensors are commonly found in heating, vents and air conditioning (HVAC) systems in both industrial and residential domains. They can be found in many other areas including hospitals, and meteorology stations to report and predict weather.

Network components – end devices (types of sensors)

- ***Pressure Sensors*** - A pressure sensor senses changes in gases and liquids. When the pressure changes, the sensor detects these changes, and communicates them to connected systems. Common use cases include leak testing which can be a result of decay. Pressure sensors are also useful in the manufacturing of water systems as it is easy to detect fluctuations or drops in pressure.
- ***Proximity Sensors*** – they are used for non-contact detection of objects near the sensor. In retail, a proximity sensor can detect the motion between a customer and a product in which he or she is interested. The user can be notified of any discounts or special offers of products located near the sensor. Proximity sensors are also used in the parking lots of malls, stadiums and airports to indicate parking availability. They can also be used on the assembly lines of chemical, food and many other types of industries.



Network components – end devices (types of sensors)

- ***Level Sensors*** - Level sensors are used to detect the level of substances including liquids, powders and granular materials. Many industries including oil manufacturing, water treatment and beverage and food manufacturing factories use level sensors. Waste management systems provide a common use case as level sensors can detect the level of waste in a garbage can or dumpster.
- **Accelerometers** – they detect an object's acceleration i.e. the rate of change of the object's velocity with respect to time. Accelerometers can also detect changes to gravity. Use cases for accelerometers include smart pedometers and monitoring driving fleets. They can also be used as anti-theft protection alerting the system if an object that should be stationary is moved.
- **Gyroscope sensors** – they measure the angular rate or velocity, often defined as a measurement of speed and rotation around an axis. Use cases include automotive, such as car navigation and electronic stability control (anti-skid) systems. Additional use cases include motion sensing for video games, and camera-shake detection systems.

Network components – end devices (types of sensors)

- ***Gas Sensors*** - These types of sensors monitor and detect changes in air quality, including the presence of toxic, combustible or hazardous gasses. Industries using gas sensors include mining, oil and gas, chemical research and manufacturing. A common consumer use case is the familiar carbon dioxide detectors used in many homes.
- ***Infrared Sensors*** - These types of sensors sense characteristics in their surroundings by either emitting or detecting infrared radiation. They can also measure the heat emitted by objects. Infrared sensors are used in a variety of different IoT projects including healthcare as they simplify the monitoring of blood flow and blood pressure. Televisions use infrared sensors to interpret the signals sent from a remote control. Another interesting application is that of art historians using infrared sensors to see hidden layers in paintings to help determine whether a work of art is original or fake or has been altered by a restoration process.

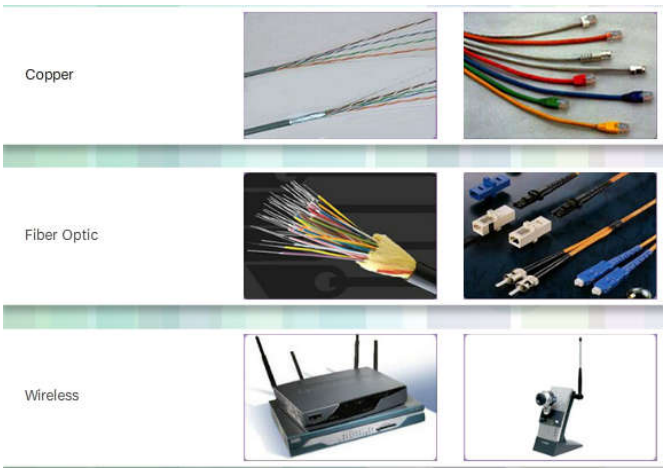
Network components – end devices (types of sensors)

- ***Optical Sensors*** – they convert rays of light into electrical signals. In the auto industry, vehicles use optical sensors to recognize signs, obstacles, and other things that a driver would notice when driving or parking. Optical sensors play a big role in the development of driverless cars. Optical sensors are very common in smart phones. For example, ambient light sensors can extend battery life. Optical sensors are also used in the biomedical field including breath analysis and heart-rate monitors.

Network components – end devices

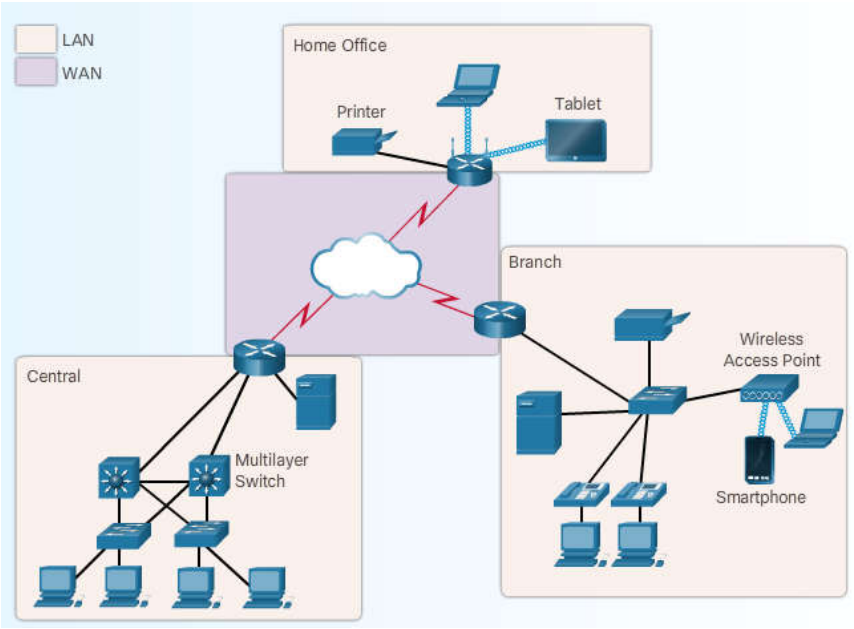
- Intermediary devices **interconnect end devices**.
- Examples of intermediary network devices are:
- *Switches and wireless access points (Network Access)*
- *Routers (Internetworking)*
- *Firewalls (Security)*

Network components – media



Network – types

- Network infrastructures can vary greatly in terms of:
- *Size of the area covered*
- *Number of users connected*
- *Number and types of services available*
- **Local Area Network (LAN)** - A network infrastructure that provides access to users and end devices in a limited area such as a home, school, office building, or campus. It provides high speed bandwidth to internal end devices and intermediary devices.
- **Wide Area Network (WAN)** - A network infrastructure that interconnects LANs over wide geographical areas such as between cities, states, provinces, countries, or continents. WANs are usually owned by an autonomous organization, such as a corporation or a government. WANs typically provide link speeds between LANs that are slower than the link speeds within a LAN.



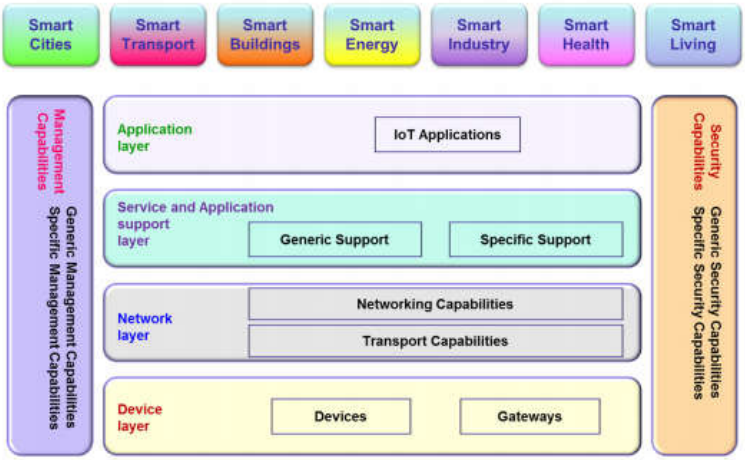
Network – types

- **Personal area network** - A personal area network is a network concerned with the exchange of information in the vicinity of a person. Typically, these systems are wireless and involve the transmission of data between devices such as smartphones, personal computers, tablet computers, etc

IoT Reference Model

- The IoT reference model is of four layers as well as management capabilities and security capabilities which are associated with the four layers.
- The four layers are as follows:
- – application layer
- – service support and application support layer
- – network layer
- – device layer.

IoT layered architecture



Iot layered architecture

- The **application layer** contains IoT applications.
- The **service support and application support layer** consists of the following two capability groupings:
- ***Generic support capabilities***: The generic support capabilities are common capabilities which can be used by different IoT applications, such as data processing or data storage. These capabilities may be also invoked by specific support capabilities, e.g., to build other specific support capabilities.
- ***Specific support capabilities***: The specific support capabilities are particular capabilities which cater for the requirements of diversified applications. In fact, they may consist of various detailed capability groupings, in order to provide different support functions to different IoT applications.

IoT layered architecture

- The network layer provides the necessary transport and networking capabilities for routing the IoT data to processing places.
- In the **device layer** lie devices (sensors, actuators, RFID devices) and gateways used to collect the sensor readings for further processing.

3.2 Communication Models

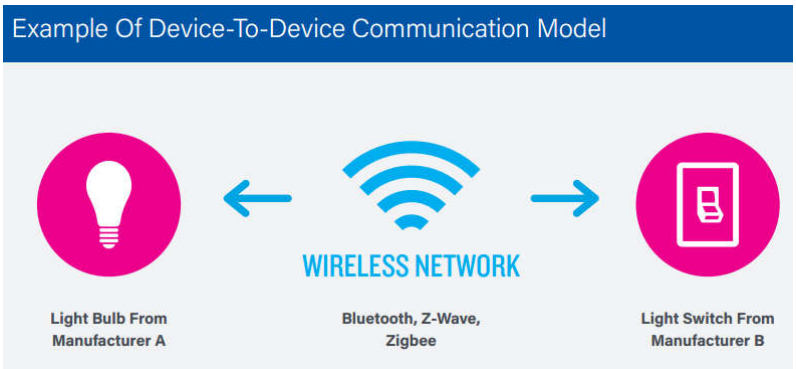
Introduction

- From an operational perspective, it is useful to think about how IoT devices connect and communicate in terms of their technical communication models.
- In March 2015, the Internet Architecture Board (IAB) released a guiding architectural document for networking of smart objects (RFC 7452), which outlines a framework of four common communication models used by IoT devices.

Device to device communication

- The device-to-device communication model represents two or more devices that **directly connect** and communicate between one another, rather than through an intermediary application server.
- These devices communicate over many types of networks, including IP networks or the Internet. Often, however these devices use protocols like **Bluetooth, Z-Wave, or ZigBee** to establish direct device-to-device communications.
- This communication model is commonly used in applications like **home automation systems**, which typically use small data packets of information to communicate between devices with relatively low data rate requirements. Residential IoT devices like light bulbs, light switches, thermostats, and door locks normally send small amounts of information to each other (e.g. a door lock status message or turn on light command) in a home automation scenario.

Device to device communication



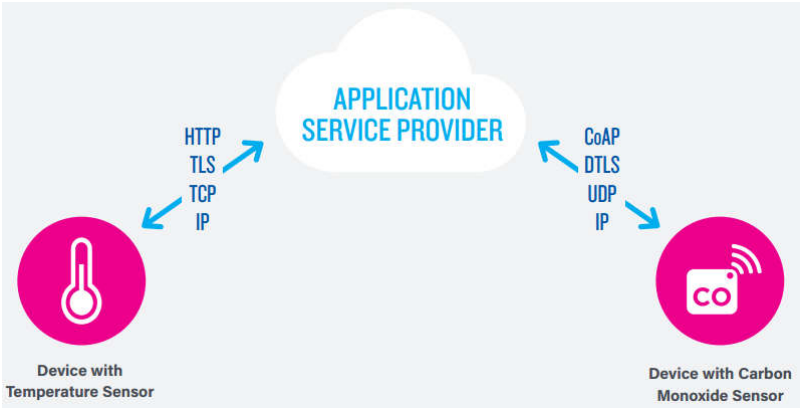
Device to cloud communications

- In a device-to-cloud communication model, the IoT device connects directly to an **Internet cloud service** like an application service provider to exchange data and control message traffic. This approach frequently takes advantage of existing communications mechanisms like traditional wired Ethernet or Wi-Fi connections to establish a connection between the device and the IP network, which ultimately connects to the cloud service.
- This communication model is employed by some popular consumer IoT devices like the Nest Labs Learning Thermostat and the Samsung SmartTV. In the case of the Nest Learning Thermostat, the device transmits data to a cloud database where the data can be used to analyze home energy consumption. Further, this cloud connection enables the user to obtain remote access to their thermostat via a smartphone or Web interface, and it also supports software updates to the thermostat. Similarly with the Samsung SmartTV technology, the television uses an Internet connection to transmit user viewing information to Samsung for analysis and to enable the interactive voice recognition features of the TV.

Device to cloud communications

- In these cases, the device-to-cloud model adds value to the end user by extending the capabilities of the device beyond its native features.
- However, interoperability challenges can arise when attempting to integrate devices made by different manufacturers. Frequently, the device and cloud service are from the same vendor. If proprietary data protocols are used between the device and the cloud service, the device owner or user may be tied to a specific cloud service, limiting or preventing the use of alternative service providers. This is commonly referred to as "**vendor lock-in**", a term that encompasses other facets of the relationship with the provider such as ownership of and access to the data. At the same time, users can generally have confidence that devices designed for the specific platform can be integrated.

Device to cloud communications



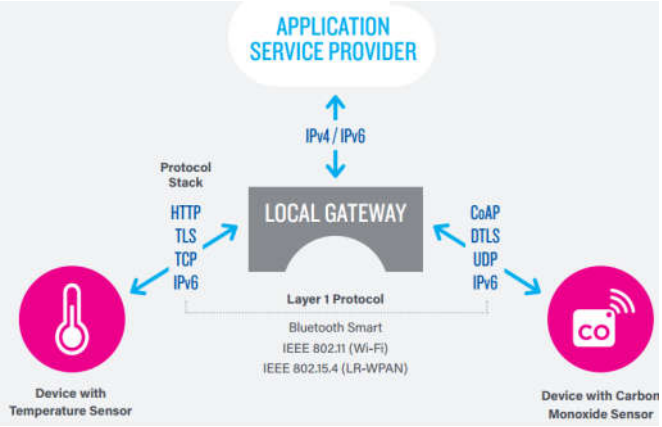
Device to GATEWAY communications

- In the device-to-gateway model, or more typically, the **device-to-application-layer gateway (ALG) model**, the IoT device connects through an ALG service as a conduit to reach a cloud service. In simpler terms, this means that there is application software operating on a local gateway device, which acts as an **intermediary between the device and the cloud service and provides security** and other functionality such as data or protocol translation.

Device to GATEWAY communications

- Several forms of this model are found in **consumer devices**.
- In many cases, the local gateway device is a **smartphone running an app to communicate with a device and relay data to a cloud service**. This is often the model employed with popular consumer items like personal fitness trackers. These devices do not have the native ability to connect directly to a cloud service, so they frequently rely on smartphone app software to serve as an intermediary gateway to connect the fitness device to the cloud.
- In other words, this communications model is frequently used to integrate new smart devices into a legacy system with devices that are not natively interoperable with them. A downside of this approach is that the necessary development of the application-layer gateway software and system adds complexity and cost to the overall system.

Device to GATEWAY communications



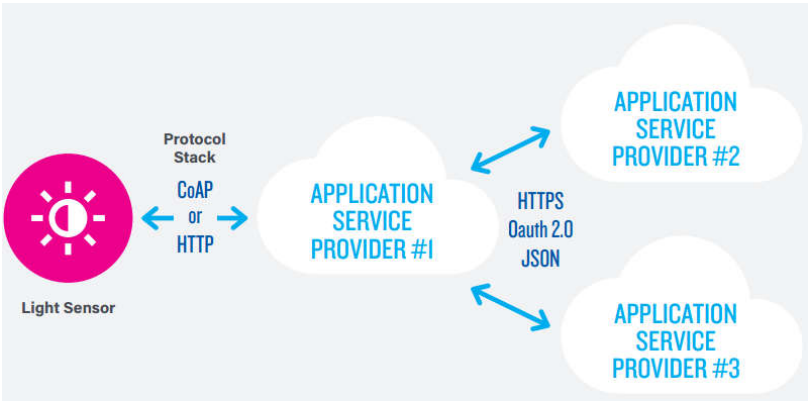
Back-end data-sharing communication

- The **back-end data-sharing model** refers to a communication architecture that enables users to ***export and analyze smart object data from a cloud service in combination with data from other sources***. This architecture supports “the [user’s] desire for granting access to the uploaded sensor data to third parties.
- This approach is an extension of the single device-to-cloud communication model, which can lead to data silos where “IoT devices upload data only to a single application service provider”. A back-end sharing architecture allows the data collected from single IoT device data streams to be aggregated and analyzed.

Back-end data-sharing communication

- For example, a corporate user in charge of an office complex would be interested in consolidating and analyzing the energy consumption and utilities data produced by all the IoT sensors and Internet-enabled utility systems on the premises. Often in the single device-to-cloud model, the data each IoT sensor or system produces sits in a stand-alone data silo.
- An effective back-end data sharing architecture would allow the company to easily access and analyze the data in the cloud produced by the whole spectrum of devices in the building. Also, this kind of architecture facilitates data portability needs. Effective back-end data-sharing architectures allow users to move their data when they switch between IoT services, breaking down traditional data silo barriers.

Back-end data-sharing communication



Chapter Review

Review

Explain the various functionalities applicable in the IoT layered architecture.

Networks are different. In what major ways to networks differ from each other?

What are the THREE major elements/components of a network?

What are the network services you expect in a small office/home office (SOHO) network?

What are the network services you expect in a medium to large-size corporate network?

Using single diagram, illustrate the major components (devices, media etc) of a LAN and WAN.

What the main disadvantage of using the device-to-gateway communication model on the IoT?