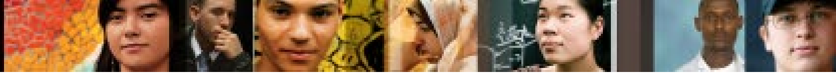
Chapter 1:
Things and Connections

IoT Fundamentals

Connecting Things 2.01

Cisco | Networking Academy®
Mind Wide Open™



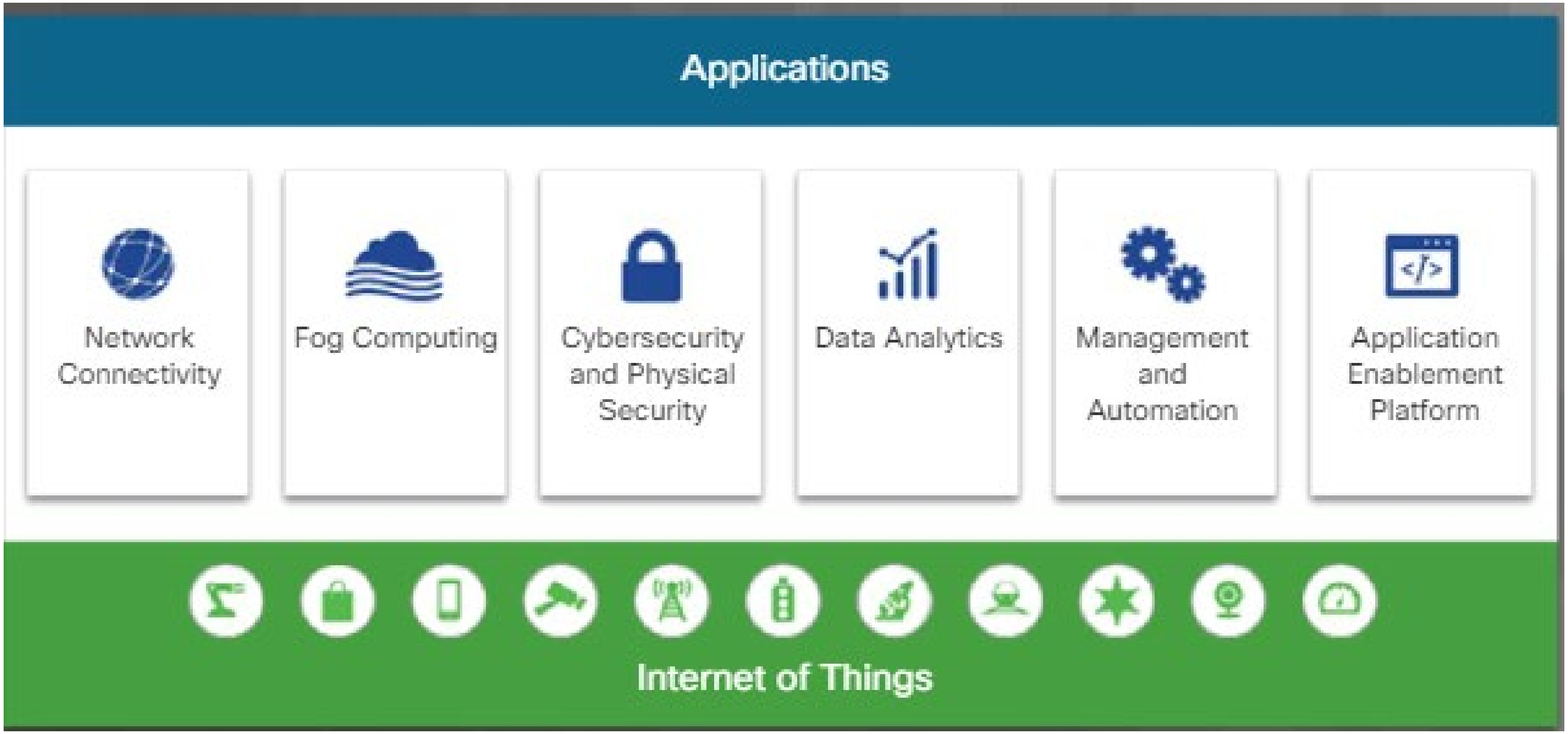
Chapter 1 - Sections & Objectives

- 1.1 What are Things?
  - Analyze the things that make up the IoT.
- 1.2 What are Connections?
  - Explain how things connect to other things and to the IoT.
- 1.3 Chapter Summary

1.1 What are Things?

Cisco | Networking Academy®
Mind Wide Open™

The Six Pillar of the IoT System


Applications
Network Connectivity
Fog Computing
Cybersecurity and Physical Security
Data Analytics
Management and Automation
Application Enablement Platform
Internet of Things

What are Things?

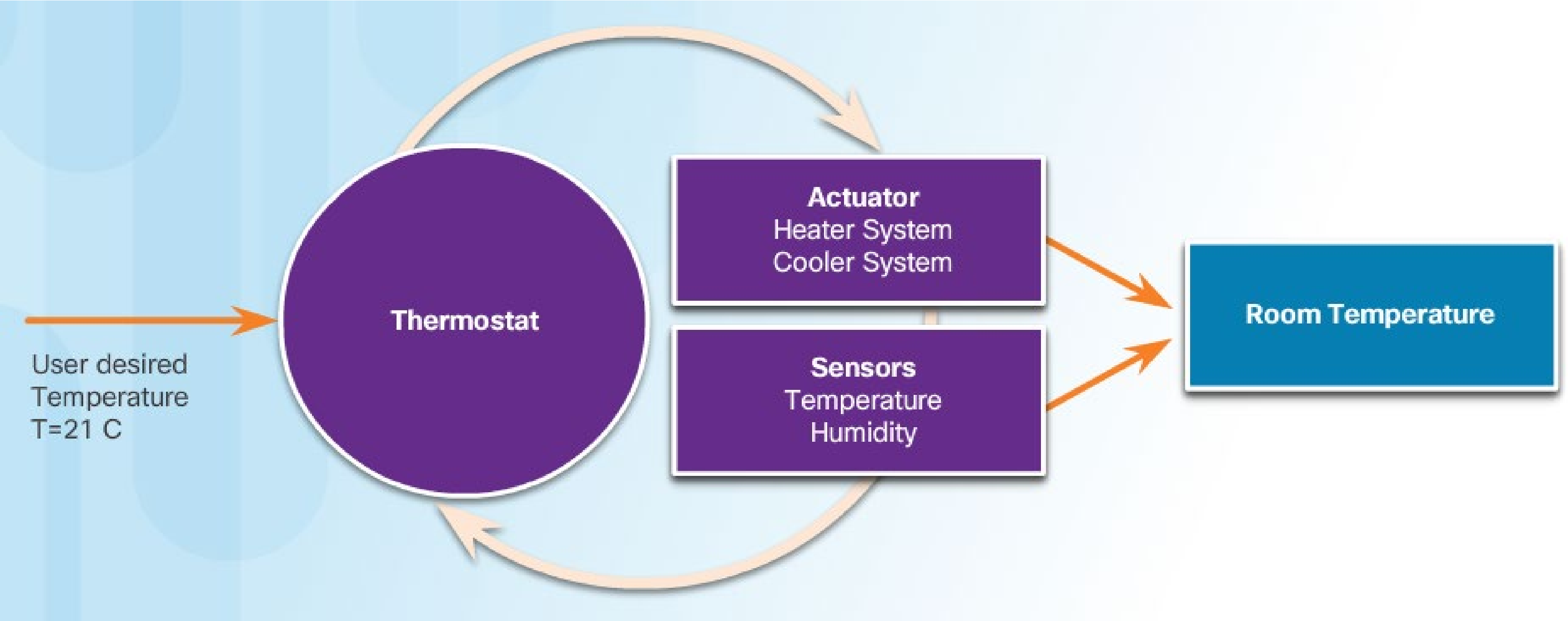
1.1.1 The Internet of Things

- The Presence of IoT in Today's World
  - The IoT is all around us.
  - The IoT helps individuals to improve quality of life.
  - The IoT also helps industries to become more efficient.
- Cisco IoT Solutions
  - The rapid IoT growth has introduced new challenges.
  - Cisco IoT System reduces the complexities of digitization.
  - Six Pillars of the Cisco IoT System are:
    - Network Connectivity
    - Fog Computing
    - Cybersecurity and Physical Security
    - Data Analytics
    - Management and Automation
    - Application Enablement Platform

What are Things?

1.1.2 Building Blocks of an IoT System

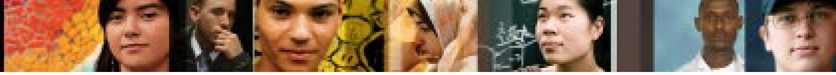
- Overview of a Controlled System
  - Feedback loops are used to provide real-time information to its controller based on current behavior.
  - In a closed loop, feedback is continuously being received by the controller from its sensors.
  - The controller continuously analyzes and processes information, and use actuators to modify conditions.



What are Things?

1.1.2 Building Blocks of an IoT System

- Sensors
  - A sensor is a device that can be used to measure a physical property by detecting some type of information from the physical world.
  - This information could be light, moisture, motion, pressure, temperature, or any other environmental condition.
  - For example, in Figure 1, the coffee farm displayed could use sensors to collect a variety of information, such as sunlight, temperature, and soil moisture. This data can then be analyzed to help maximize the yield and quality of coffee beans.



What are Things?

1.1.2 Building Blocks of an IoT System

- There are many types of sensors. Figure 2 displays examples of sensors.
- A sensor may be connected to a controller either directly or remotely. Sensors and controllers are usually connected by means of analog or digital circuits. Sensors send data to a controller. That controller could react to the sensor data immediately and change the actuator settings. As an example, a Controller Area Network (CAN) is a standard used in most modern automobiles to allow for communication between sensors and controllers without any host computers. Most new cars are equipped with backup cameras or anti-collision sensors. These cameras and their sensors can alert the microcontrollers if an object is in the way and the microcontrollers will automatically cause the car to emit a warning signal or to apply the brakes.
- The controller may also act as a gateway to an IP network and pass the sensor data to be stored or analyzed on servers in the fog or the cloud. The collected data and analyses can be used to trigger actions by people, systems, or machines. As examples, the quantity of cars on the road may cause a change to the traffic light system. The analysis of birth rates in different counties may cause a government to build a new school in a different location.

Various Types of Sensors

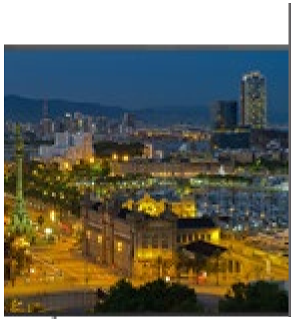
What are Things?

1.1.2 Building Blocks of an IoT System

- Figure 3 provides examples of how sensors are used in various industries. Click each to see what these sensors measure.

Oil, Gas, Mining

Sensors detect chemical levels such as carbon monoxide, carbon dioxide, oxygen, methane, hydrogen, ammonia, and hydrogen sulfide.



Cities

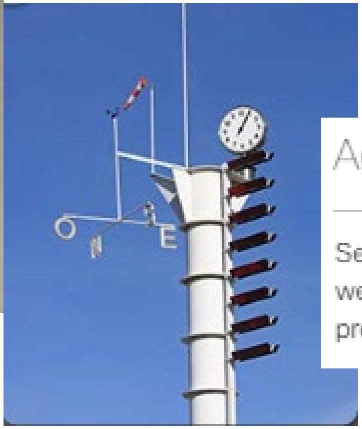
Some sensors include pressure (for parking), dust concentrations, noise, displacement of cracks, temperature, humidity, and luminosity.

Transportation

Sensors measure idle times, fuel usage, engine faults, and engine load.

Utilities

Sensors measure current, levels, flows, temperature, humidity, and luminosity.



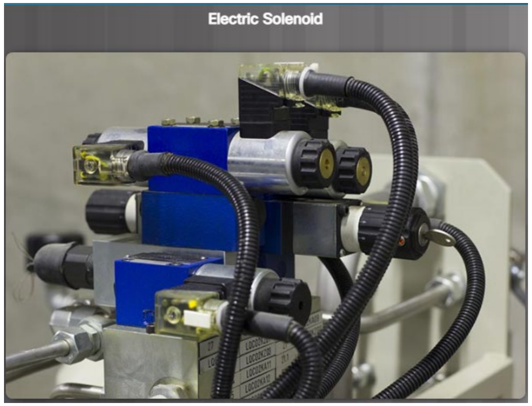
Agriculture

Sensors detect soil moisture, leaf wetness, solar radiation, atmospheric pressure, and stem diameter.

What are Things?

Building Blocks of an IoT System (Cont.)

- Actuators
  - An actuator is a basic motor that can be used to control a system.
  - Can be **hydraulic**, **electric** or **pneumatic**.
  - can be responsible for transforming an electrical signal into physical output.
  - The example in the figure displays an industrial actuator consisting of an electric solenoid used to control hydraulics.
  - In other areas, an actuator can be responsible for transforming an electrical signal into physical output. This physical output could provide information to a user via LEDs or modify another device or environment. For example, the heater in the thermostat feedback loop is an actuator because it changes the status of the controlled environment (temperature) in response to an electrical signal.
  - Regardless of how the actuator causes the movement to be performed, the basic function of an actuator is to receive a signal from the controller, and based on that signal, perform a set action.



What are Things?

Building Blocks of an IoT System (Cont.)

- Controllers
  - Responsible for collecting data from sensors and providing network connectivity.
  - Controllers may have the ability to make immediate decisions.
  - May also send data to remote and more powerful computer for analysis.
  - This more powerful computer might be in the same LAN as the controller or might only be accessible through an Internet connection.

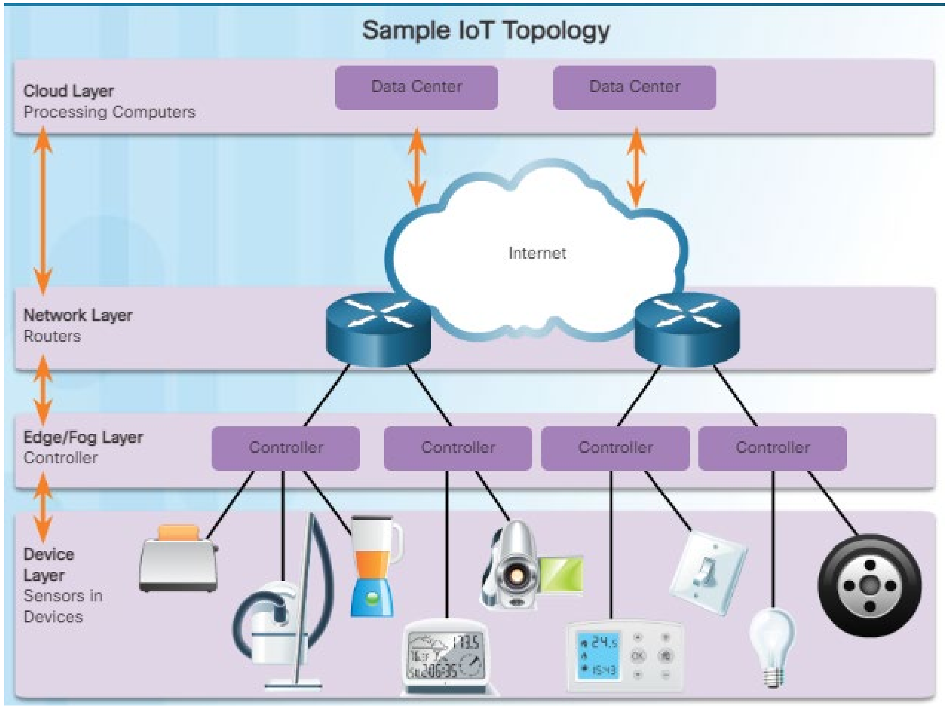


Figure 1

Figure 1 displays a sample IoT topology consisting of **sensors**, **controllers**, **routers** and **data centers**. To reach the more powerful computers in the data center, the controller will first send data to a local router. This router is the interface between the local network and Internet. It can send data back and forth between them.

Sample of IoT Topology in Fog Computing

- Figure 2 displays a sample IoT topology that highlights how controllers are used in fog computing. Imagine smart traffic lights that contain sensors and actuators. The sensors detect and report traffic activity to the controller. The controller is able to process this data locally and determine optimal traffic patterns. Using this information the controller will send signals to the actuators in the traffic lights to adjust traffic flows. This is an example of machine-to-machine (M2M) communication. In this scenario, the sensors, actuators, and the controller all exist within the fog. That means that the information is not sent beyond the local network of end devices.

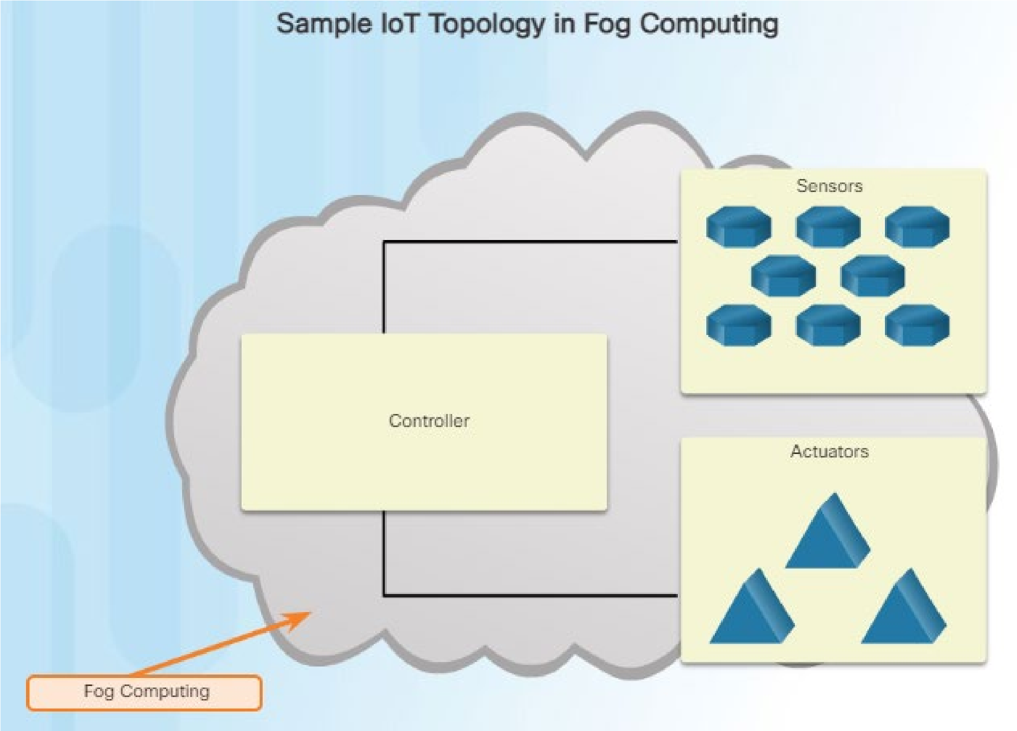


Figure 2

Sample IP-Enabled Controller Topology

- Figure 3 displays an example of IP-enabled controllers. The IP-enabled controller forwards information across an IP network, and allows individuals to access the controller remotely. In addition to forwarding basic information in an M2M configuration, some controllers are able to perform more complex operations. Some controllers can consolidate information from multiple sensors or perform basic analysis of data received.

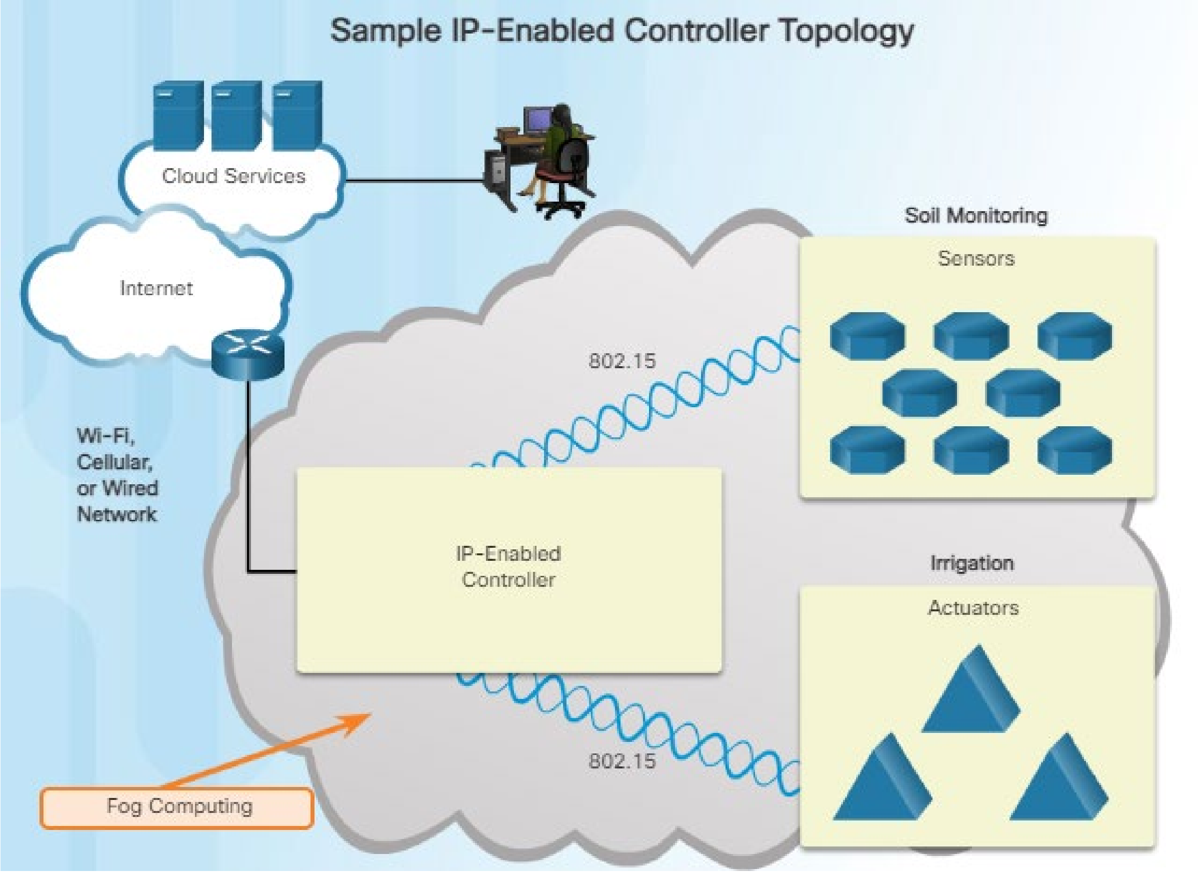


Figure 3

- The Arduino microcontroller, shown in Figure 4, and the Raspberry Pi (RaPi), shown in Figure 5, are both types of controllers. They can both operate without the Internet and are used by hobbyists and professionals. The key difference between the two is physical size, available processing power, memory, and OS. Typically the Arduino requires less power than the RaPi and is more suitable for analog input. The application should dictate which controller is the best to use.
- The two controllers are commonly used together. For instance, you can acquire data with the Arduino and then process the data using the Raspberry Pi. More details about the Arduino and Raspberry Pi controllers will be covered in a later chapter.

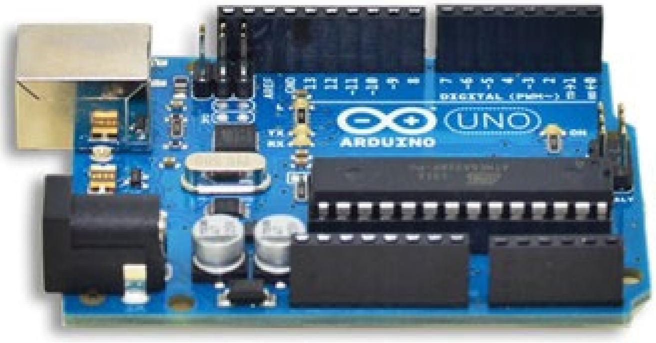


Figure 4

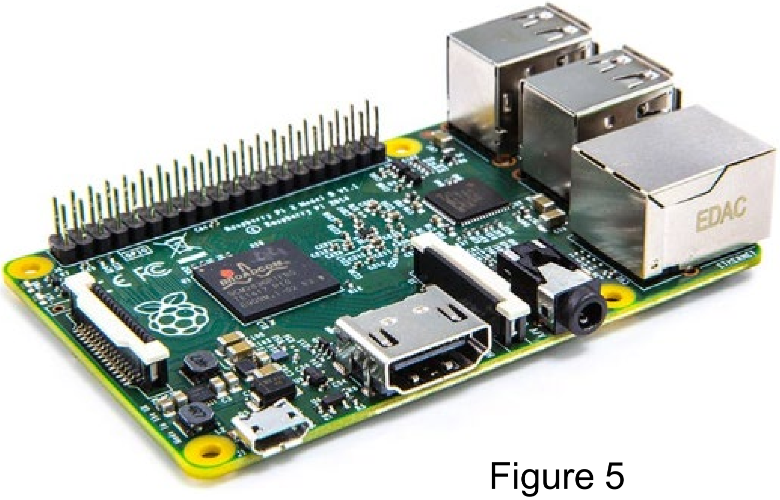
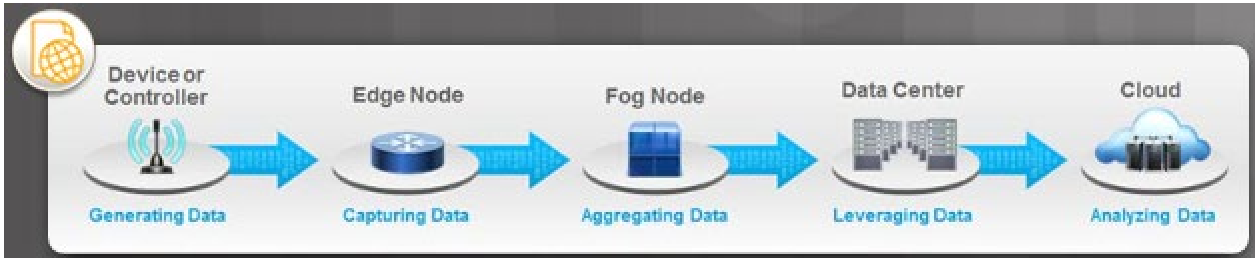


Figure 5

Building Blocks of an IoT System (Cont.)

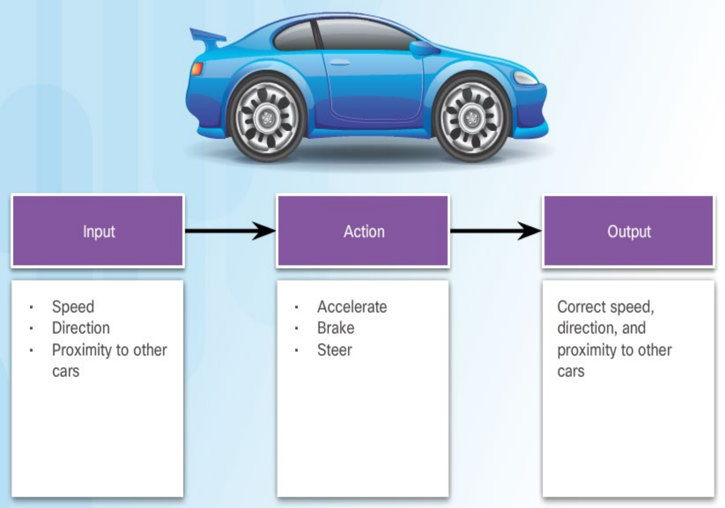
IoT Process Flow



- Key components of some of the simplest IoT systems include sensors connecting, through **a wireless or wired connection**, to actuators or controllers. As with many components in any system, **some devices can have more than one function**. This is the case for the controller in an IoT System. A controller can collect data from sensors without human intervention or network connectivity. As an example, a sensor determines that the temperature in an apartment has dropped below a pre-set level. The controller will process the data and send output to cause the heater (the actuator) to turn on.
- A controller may also act as a gateway to the local network. In the previous example, if the IoT system is designed to capture the temperature changes within every apartment of the building, the controller may pass the data up to be stored or analyzed on servers in the local or edge network. Where the data is processed will impact the speed in which change can take place in the system. Data can be stored and processed on devices that are near the edge of the network or even closer to the sensors. This type of processing is called fog computing. Fog nodes that create areas for processing are part of this system.
- A controller may also be a gateway to a cloud network. If the IoT system from our initial example is designed to aggregate the thermostat data from several different apartment buildings owned by the same company, multiple controllers and devices may store and process the sensor data in different fog nodes. The data from different fog nodes would be stored, aggregated, and analyzed. This analyzed data could then be used to make informed business decisions.

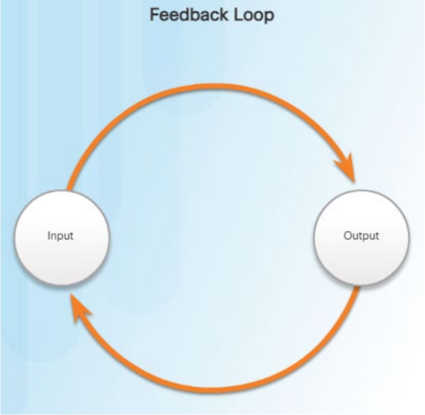
What are Things?

1.1.3 Processes in Controlled Systems



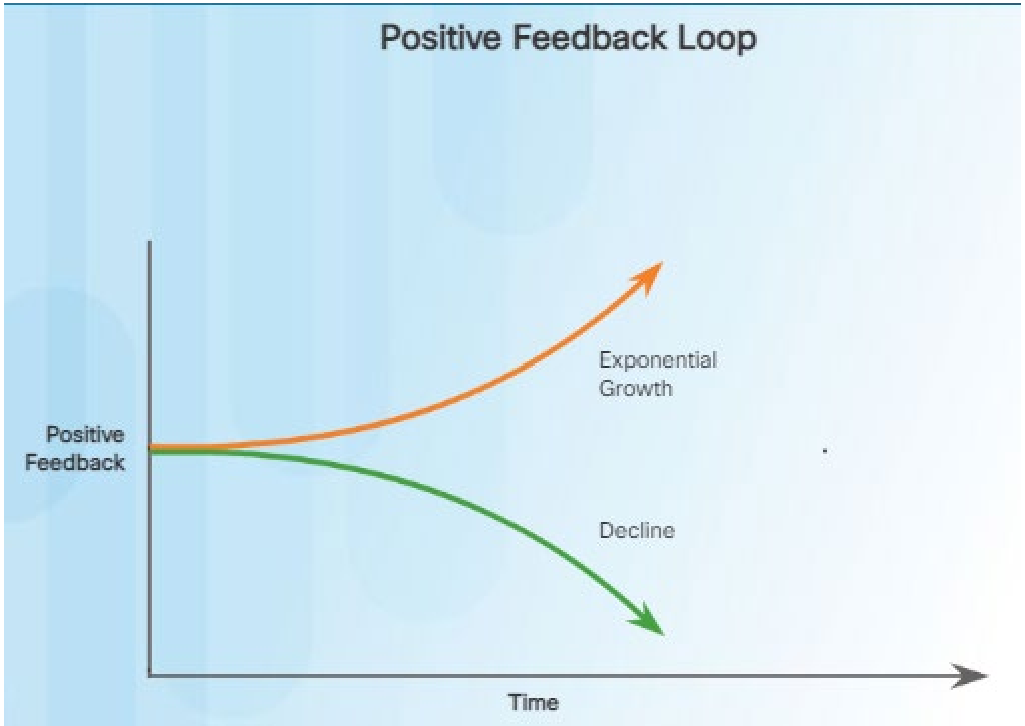
- Processes
  - A process is a series of steps or actions taken to achieve a desired result by the consumer of the process.
  - As illustrated in Figure 1, a process uses inputs to execute the right actions to achieve the desired output. More formally, a process is a series of steps or actions taken to achieve a desired result by the consumer of the process. A system is a set of rules that govern the series of steps or actions in the process.
  - Driving a car is an example of a process. Example inputs include speed, direction, and proximity to other cars. Example actions include accelerating, braking, and steering the car. All of these actions create a system, known as driving. Example outputs would be the correct speed, direction, and proximity to other cars and obstacles, as highlighted in Figure 2.

1.1.3 Processes in Controlled Systems



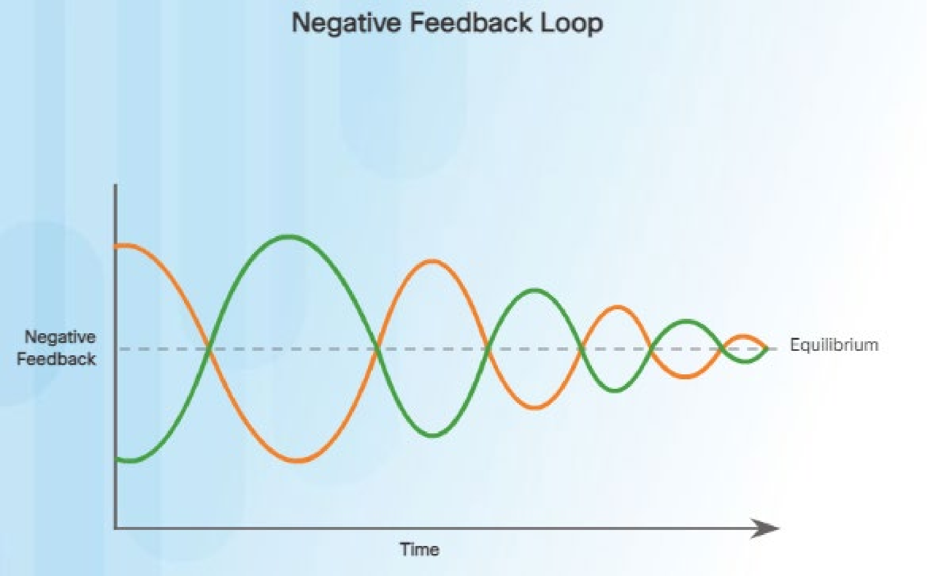
- Feedback
  - Feedback is when the output of a process affects the input. To illustrate this, consider how feedback was used to safely land on the moon (Figure 1). The computer continually received altitude and speed feedback measurements and displayed this information to the astronaut and on-board systems. The astronaut used the feedback to control the spacecraft and adjust altitude, engine, and thrust levels to successfully land on the moon.
  - Feedback is often referred to as a feedback loop. This is because the input results in output that is continually resampled and used as new input, as illustrated in Figure 2. The feedback loop represents the idea of a cause-and-effect cycle, or circuit, where results continually adjust action.
  - Feedback loops can be positive or negative.
  - Feedback is when the output of a system, or process, affects the input.
  - Many system processes normally have some type of feedback loop mechanism. Systems usually have a way of looping or feeding back information about the quality of the output.

Positive Feedback

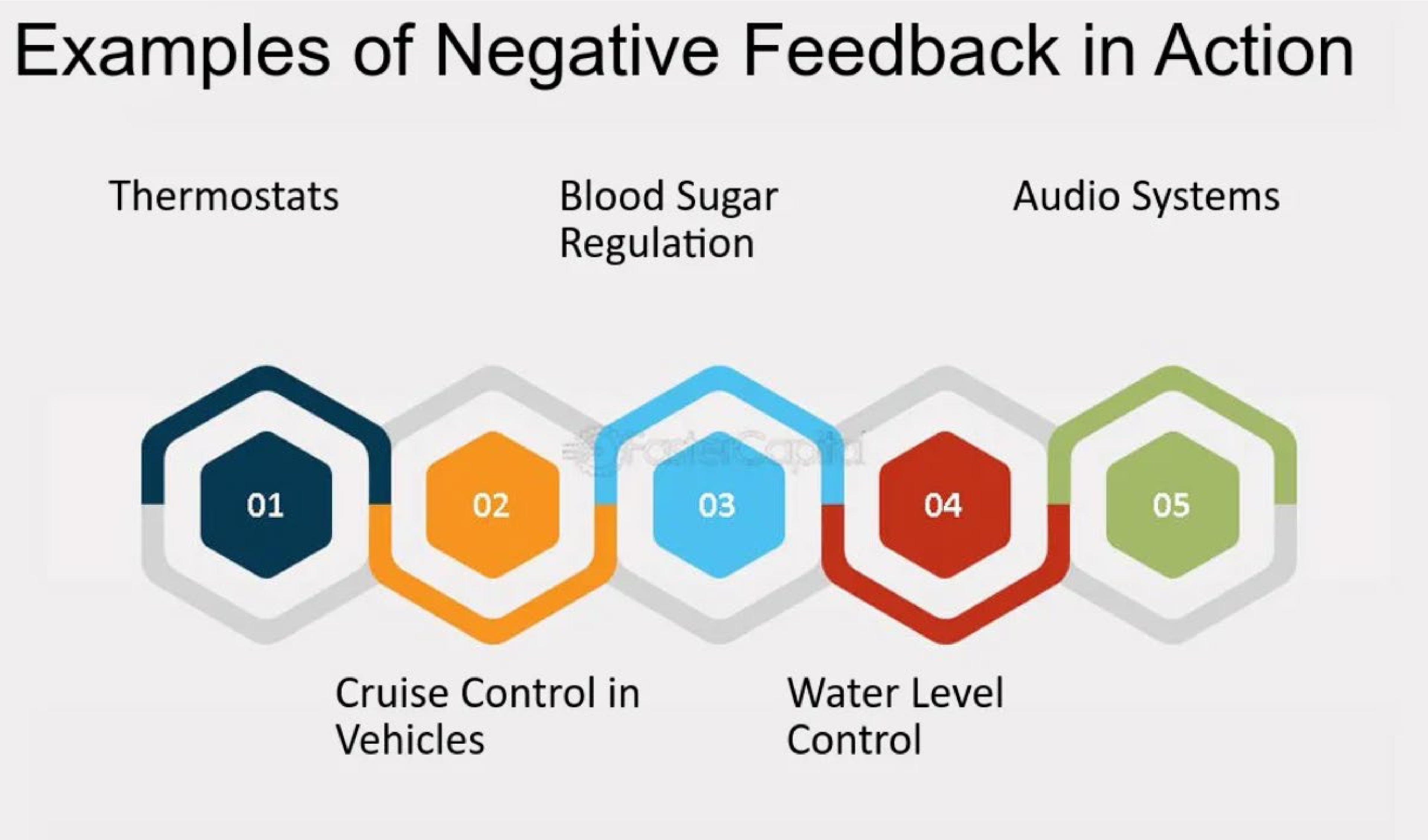


- Feedback reinforces the original input. Positive feedback accelerates the transformation of the output in the same direction as the previous result. It tends toward either exponential growth or decline, as shown in the Figure.

Negative Feedback



- Feedback cancels out or counteracts the original input. Negative feedback diminishes the effect of the previous result. It tends towards stabilization, reaching some level of equilibrium, as shown in the Figure.



Examples of Negative Feedback in Action

01 Thermostats

02 Cruise Control in Vehicles

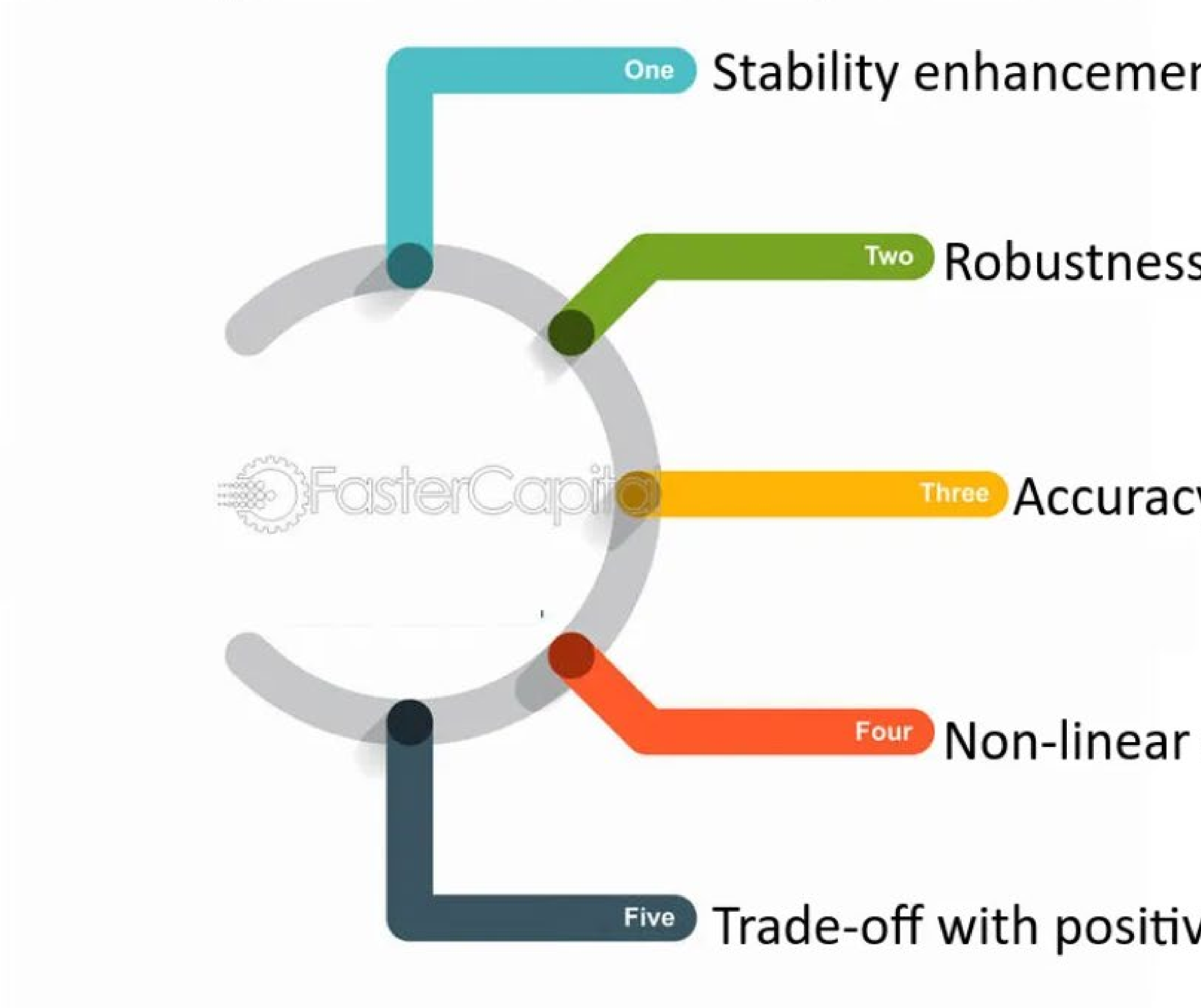
03 Blood Sugar Regulation

04 Water Level Control

05 Audio Systems

https://fastercapital.com/

How Negative Feedback Optimizes Control Systems



One Stability enhancement

Two Robustness against disturbances

Three Accuracy and precision

Four Non-linear system control

Five Trade-off with positive feedback

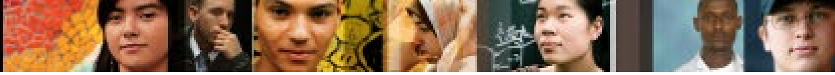
https://fastercapital.com/

What are Things?

1.1.3 Processes in Controlled Systems

- Control Systems
  - Includes a controller that uses inputs and outputs to manage and regulate the behavior of the system in an attempt to achieve a desired state.

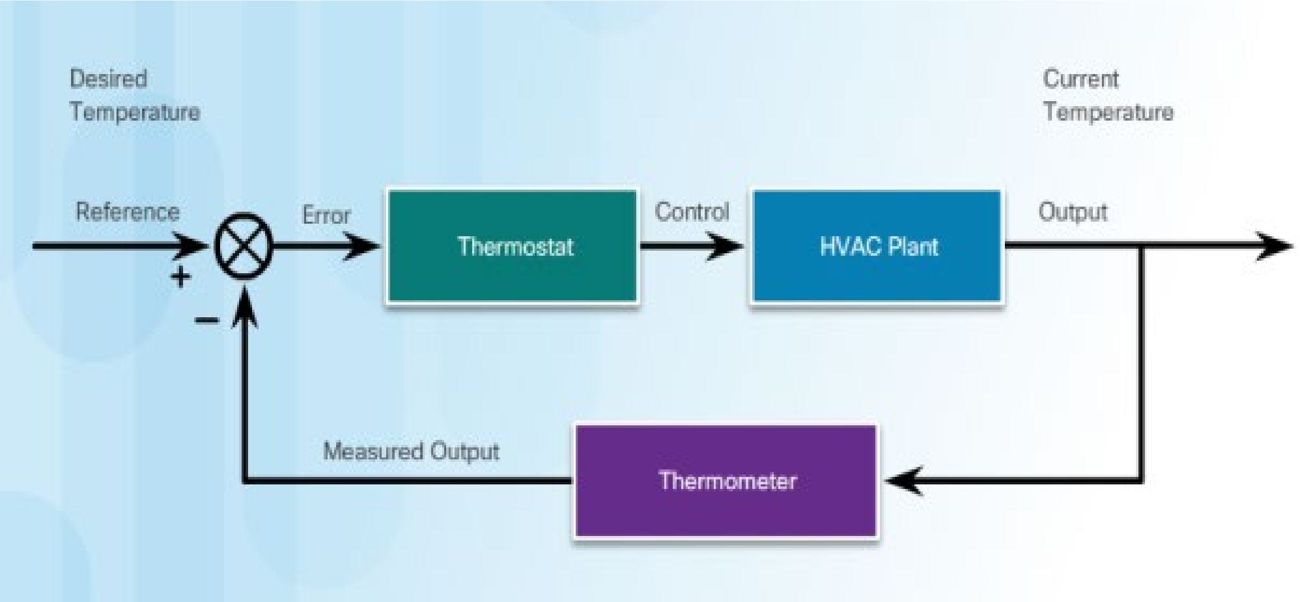
  - The controlled portion of the system is often called the plant.
  - Choosing the adjustments to apply to a plant to achieve a desired output is called control theory.
  - Control theory is applied to many systems, including driving a car.
  - https://www.youtube.com/watch?v=O-OqgFE9SD4 (explanation on open-loop and closed-loop control system)



- A control system includes a controller that uses inputs and outputs to manage and regulate the behavior of the system in an attempt to achieve a desired state. The input specifies what the output should be for the whole process. The controller indicates what specific changes are needed to achieve the desired output based on the input. The controlled portion of the system, the process and the actuator, is often called the plant. The input is used by the plant to produce the desired output.
- Choosing the adjustments to apply to a plant to achieve a desired output is called control theory. Control theory is essentially a strategy to select the correct input and how to go about generating the desired output.
- Control theory is applied in all types of devices. Consider how control theory is applied when driving a car. The driver of the car is the controller, managing and regulating the car (the plant). Based on the input, the driver determines how to use each control (e.g., accelerator, brake, steering wheel) to achieve the intended output. Many of the processes in a car also depend on control systems designed by the automobile manufacturer. In these control systems, the output is measured using some type of sensor to inform what changes a controller needs to make. The goal is to design a system with an error rate of zero. This means that the output of the plant is exactly what you want it to be. Therefore, if a driver wants to travel at 65 MPH, then setting the cruise control to 65 MPH should achieve exactly that result.
- On a greater scale of technology, consider how control theory was applied to successfully land the NASA Curiosity Rover on Mars. The rover used a dynamic control system to determine how to move through space. The rover sensors provided input by repeatedly sampling its position and velocity during its descent to the surface of Mars. Processes in the rover used this input to make the necessary adjustments to land at the intended destination.
- Control systems can be open-loop or closed-loop systems. The difference between these two systems is based on whether it uses feedback or not.

Processes in Controlled Systems (Cont.)

- Open-Loop Control Systems
  - Open-loop control systems do not use feedback.
  - The plant performs a predetermined action without any verification of the desired results.
  - Open-loop control systems are often used for simple processes.
- Closed-Loop Control Systems
  - A closed-loop control system uses feedback to determine whether the collected output is the desired output.
  - The result is then fed back into a controller to adjust the plant for the next iteration of output, and the process repeats.

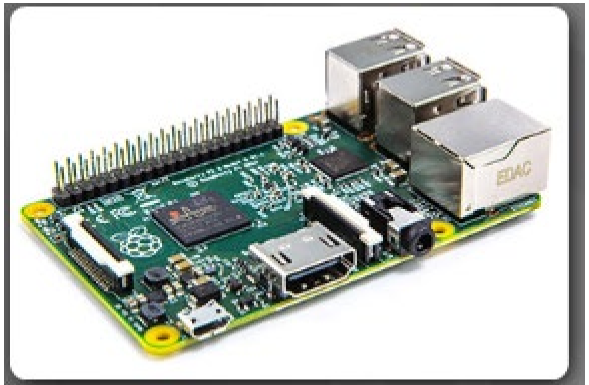


What are Things?

Processes in Controlled Systems (Cont.)

- Closed-Loop Controllers
  - There are many types of closed-loop controllers:
    - **Proportional controllers** (P): based on the difference between the measured output and the desired output.
    - **Integral controllers** (PI): use historical data to measure how long the system has deviated from the desired output.
    - **Proportional, Integral and Derivative controllers** (PID): include data about how quickly the system is approaching the desired output.
    - PID controller is an efficient way to implement feedback control.
    - The Arduino and Raspberry Pi devices can be used to implement PID controllers.

Arduino (Microcontroller)



Raspberry Pi (Computer)

Interdependent System

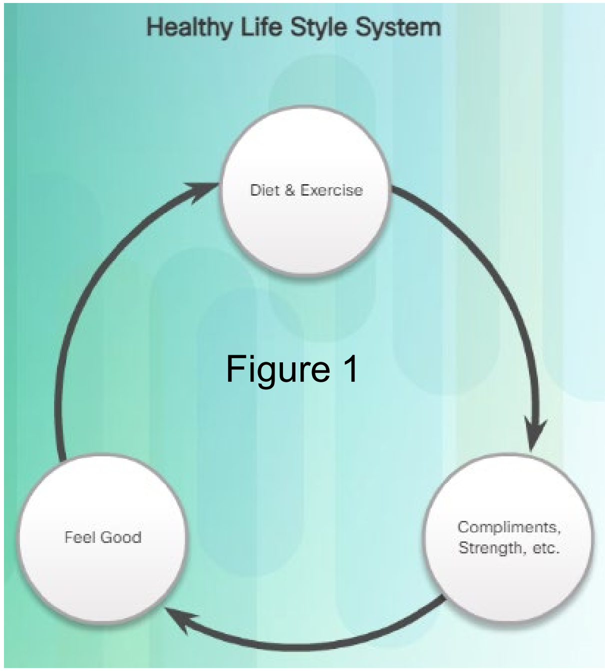


Figure 1

- Closed-loop control systems are simple to understand.
- However, there can be considerable complexity in the real world. Many factors can impact systems, and the extent of their impact is not always easily measured. Most systems have many interdependent pieces contributing to and affecting the output.
- For example, consider a healthy lifestyle system, as shown in the diagram in Figure 1. A person embarks on a program of diet and exercise. After a short time, they become stronger and their clothes fit more loosely. They begin to receive compliments (feedback) from others. This results in good feelings that motivate them to continue their diet and exercise.

Interdependent System (cont..)

- Another example is the Earth's climate system. The diagram in Figure 2 shows how rising global temperatures cause arctic ice to melt faster, thereby increasing the amount of ocean surface. Increased ocean surface means less sunlight is reflected back into space, which increases the temperature of the earth.
- Finally, consider the example of recycling materials back into the supply chain. Click https://www.environmentalleader.com/2014/05/dell-builds-pc-from-recycled-plastic-electronics/ : to learn about how Dell is recycling the plastic from old electronics back into the supply chain, which is used to manufacture new computer systems.

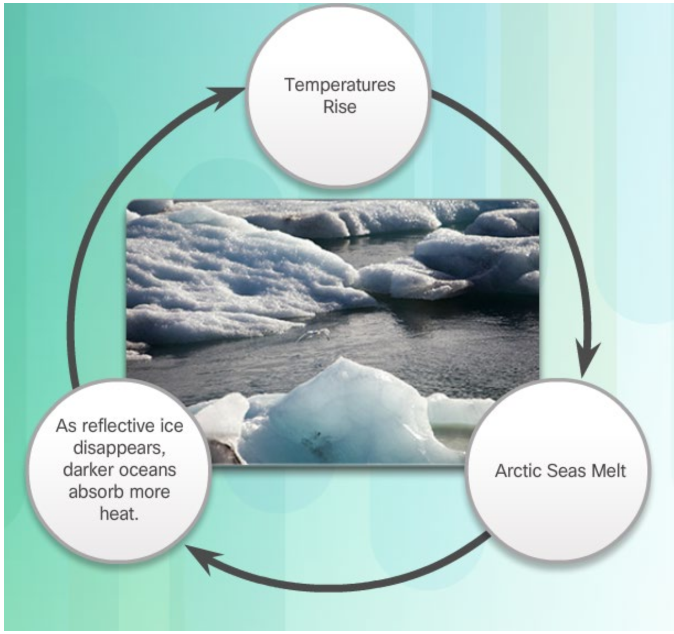

Temperatures Rise
Arctic Seas Melt
As reflective ice disappears, darker oceans absorb more heat.

Figure 2

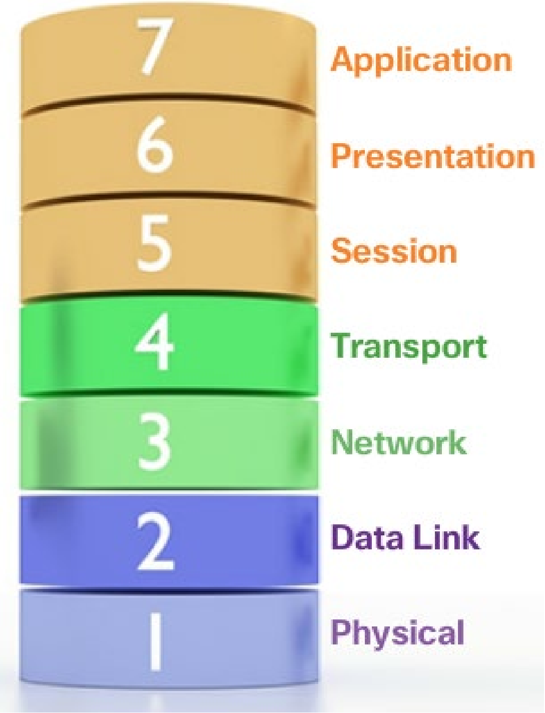
1.2 What are Connections?

Cisco | Networking Academy®
Mind Wide Open™

What are Connections?

1.2.1 Models of Communication

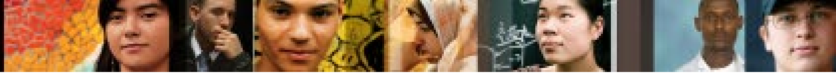
- Models of Communication
  - Layered networking models are used to illustrate how a network operates. There are many benefits to using a layered model to explain network protocols and operations:
  - They assist in protocol design because protocols that operate at a specific layer have defined information that they act upon and a defined interface to the layers above and below.
  - They foster competition because products from different vendors can work together.
  - They prevent technology or capability changes in one layer from affecting other layers above and below.
  - They provide a common language to describe networking functions and capabilities.



What are Connections?

1.2.1 Models of Communication (cont'd)

- **Standardization**
  - The challenge for the IoT is to ensure these emerging IoT devices can connect securely and reliably to the Internet and to each other.
  - Consistent, secure, and commonly recognized technologies and standards is needed.
  - Organizations such as the Industrial Internet Consortium, OpenFog Consortium, and the Open Connectivity Foundation, are helping to develop standard architectures and frameworks.
  - Each day more and more devices are coming online, adding to the ever-growing IoT. Analysts agree the IoT will grow to many billions of devices over the next decade. The challenge for the IoT ecosystem is to ensure these emerging IoT devices can connect securely and reliably to the Internet and to each other.
  - Ensuring effective communications across diverse IoT systems requires the use of consistent, secure, and commonly recognized technologies and standards. The networking industry has developed layered models such as the OSI and the TCP/IP models to structure and standardize connectivity amongst networking devices. With the explosion of IoT devices connecting and communicating over the Internet, it is even more critical that these devices are also able to connect and communicate regardless of the manufacturer of the device or the operating system on which it runs.

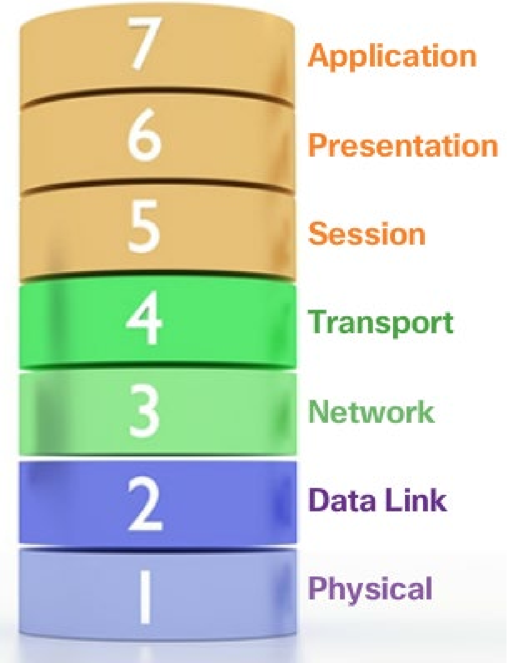


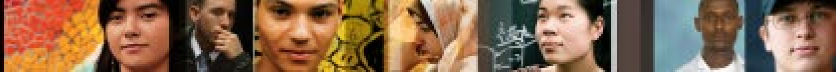
Standardization

- Many new organizations such as the Industrial Internet Consortium, OpenFog Consortium, and the Open Connectivity Foundation, are working with members from industry, government, and academia to support and encourage the creation and adoption of new IoT systems. To assist in this goal, they are helping to develop standard architectures and frameworks that will allow devices to connect and communicate reliably and safely in the IoT.
- The Industrial Internet Consortium (IIC) has used workgroups with representatives from industries such as energy, manufacturing, transportation, and healthcare, to create the Industrial Internet Reference Architecture. This architecture is a standards-based architectural template and methodology for the industrial IoT. The IIC is also collaborating with companies such as Cisco, Bosch Rexroth, Intel, and National Instruments to develop the world's first Time Sensitive Networking (TSN) testbed. The goal of the testbed is to display the value of new Ethernet standards required to support seamless interoperability among the emerging smart devices required for new IoT systems. The testbed will provide feedback to relevant standards organizations on areas for consideration and improvement.
- The OpenFog Consortium is creating an open reference architecture for fog computing. They also build operational models and testbeds, define and advance technology, educate the market, and promote business development through an OpenFog ecosystem.
- The Open Connectivity Foundation (OCF) is working towards the creation of solutions that map to a single, open IoT interoperability specification. To that end, the OFC has sponsored the IoTivity Project, an open source software framework. This framework enables seamless connectivity for devices such as appliances, phones, computers, and industrial equipment. These devices will be able to communicate with one another regardless of manufacturer, operating system, or chipset.

Models of Communication (Cont.)

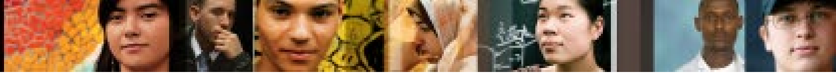
- TCP and OSI Models
  - Both OSI and TCP/IP models are used to describe network connections and often used interchangeably.
  - The TCP/IP model is commonly referred to as the Internet model.
  - The OSI model provides an extensive list of functions and services that can occur at each layer.
- IoT World Forum Reference Model
  - Developed as a common framework to guide and to help accelerate IoT deployments.
  - It's intent is to provide common terminology and help clarify how information flows and is processed for a unified IoT industry.





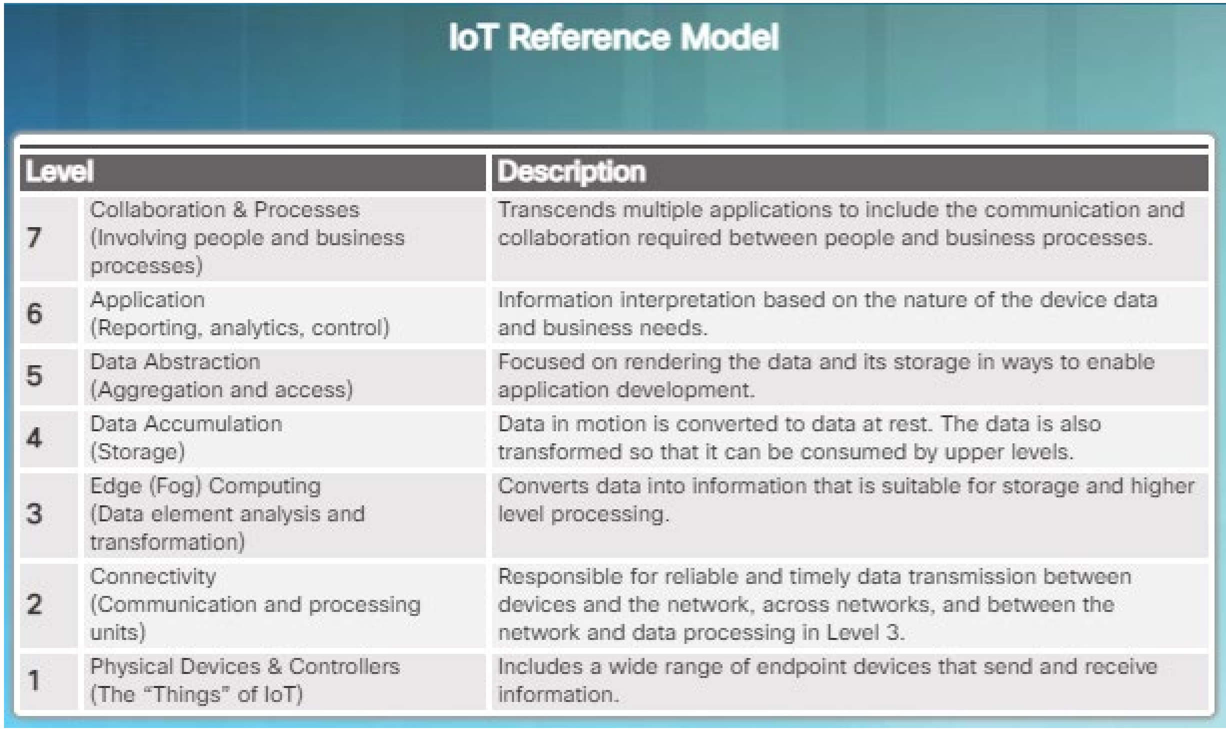
(elaboration)

- Network connections are most often described as using the OSI and TCP/IP models. As shown in Figure 1, both models use layers, and each layer has a function.
- The TCP/IP protocol model for internetwork communications was created in the early 1970s. As shown in Figure 2, it defines four categories of functions that must occur for communications to be successful. The architecture of the TCP/IP protocol suite follows the structure of this model which is why it is called a protocol model. The TCP/IP protocol model is commonly referred to as the Internet model.
- The OSI reference model provides an extensive list of functions and services that can occur at each layer. It also describes the interaction of each layer with the layers directly above and below. Click each layer of the OSI model in Figure 3 to view the details.
- It is important to note that in networking, both models are often used interchangeably. Therefore, it is a good idea to make sure you are familiar with these models.
- **Note**: Whereas the TCP/IP model layers are referred to only by name, the seven OSI model layers are more often referred to by number rather than by name. For instance, the physical layer is referred to as Layer 1 of the OSI model.



IoT World Forum Reference Model

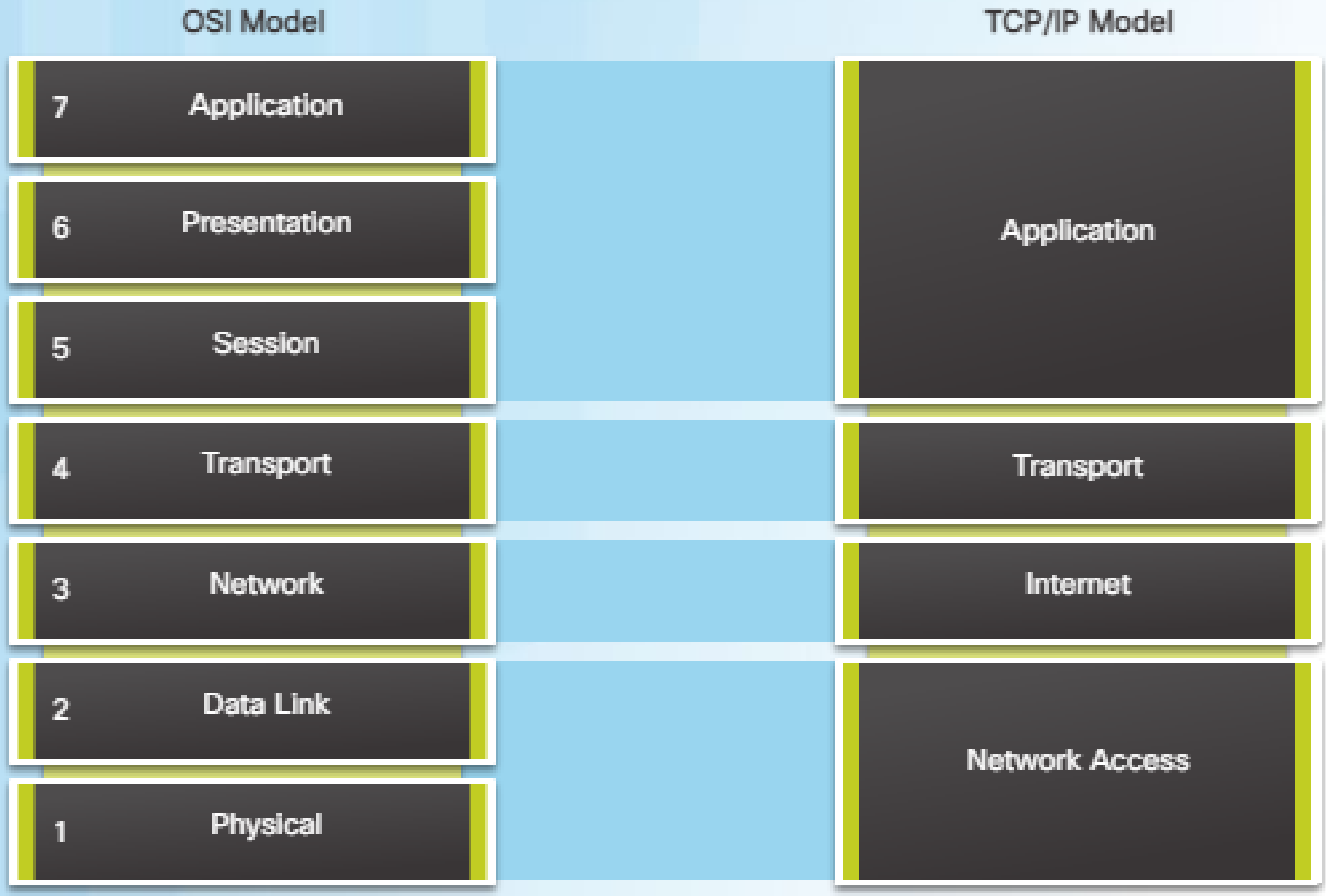
- Like the OSI model, the IoT Reference Model has seven parts. However, the parts are called levels instead of layers. The IoT reference model was developed as a common framework to guide and to help accelerate IoT deployments. The model is the result of a collaborative effort of the 28 members of the IoT World Forum's Architecture, Management and Analytics Working Group. It is also endorsed by the Industrial Internet Consortium (IIC).
- The intent of the IoT reference model is to provide common terminology and help clarify how information flows and is processed for a unified IoT industry.
- As shown in the figure, the model breaks down the IoT concept into seven functional levels, from physical devices and controllers at Level 1 to collaboration and processes at Level 7.



IoT Reference Model

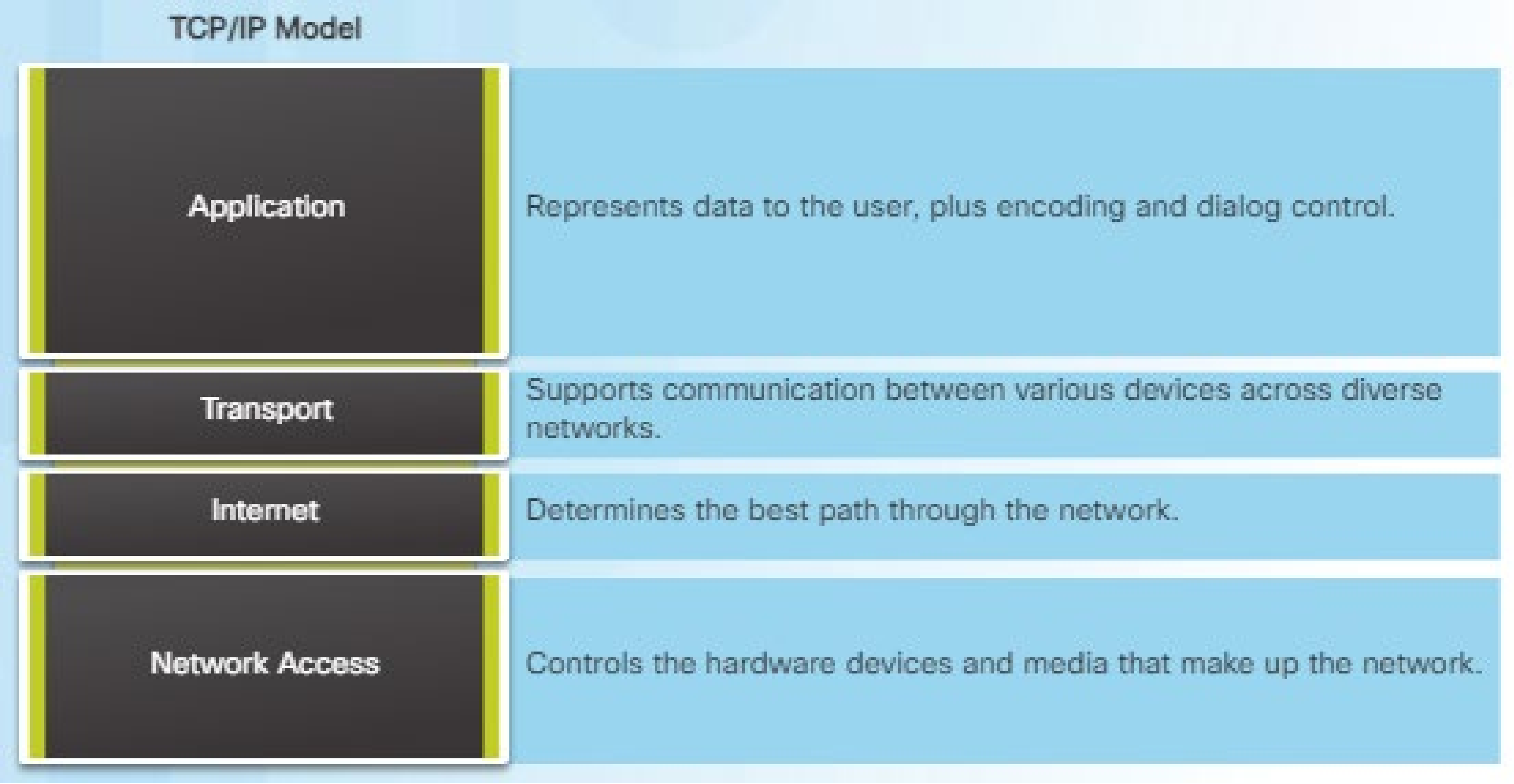
Level		Description
7	Collaboration & Processes (Involving people and business processes)	Transcends multiple applications to include the communication and collaboration required between people and business processes.
6	Application (Reporting, analytics, control)	Information interpretation based on the nature of the device data and business needs.
5	Data Abstraction (Aggregation and access)	Focused on rendering the data and its storage in ways to enable application development.
4	Data Accumulation (Storage)	Data in motion is converted to data at rest. The data is also transformed so that it can be consumed by upper levels.
3	Edge (Fog) Computing (Data element analysis and transformation)	Converts data into information that is suitable for storage and higher level processing.
2	Connectivity (Communication and processing units)	Responsible for reliable and timely data transmission between devices and the network, across networks, and between the network and data processing in Level 3.
1	Physical Devices & Controllers (The "Things" of IoT)	Includes a wide range of endpoint devices that send and receive information.

Comparing the OSI Model and the TCP/IP Model



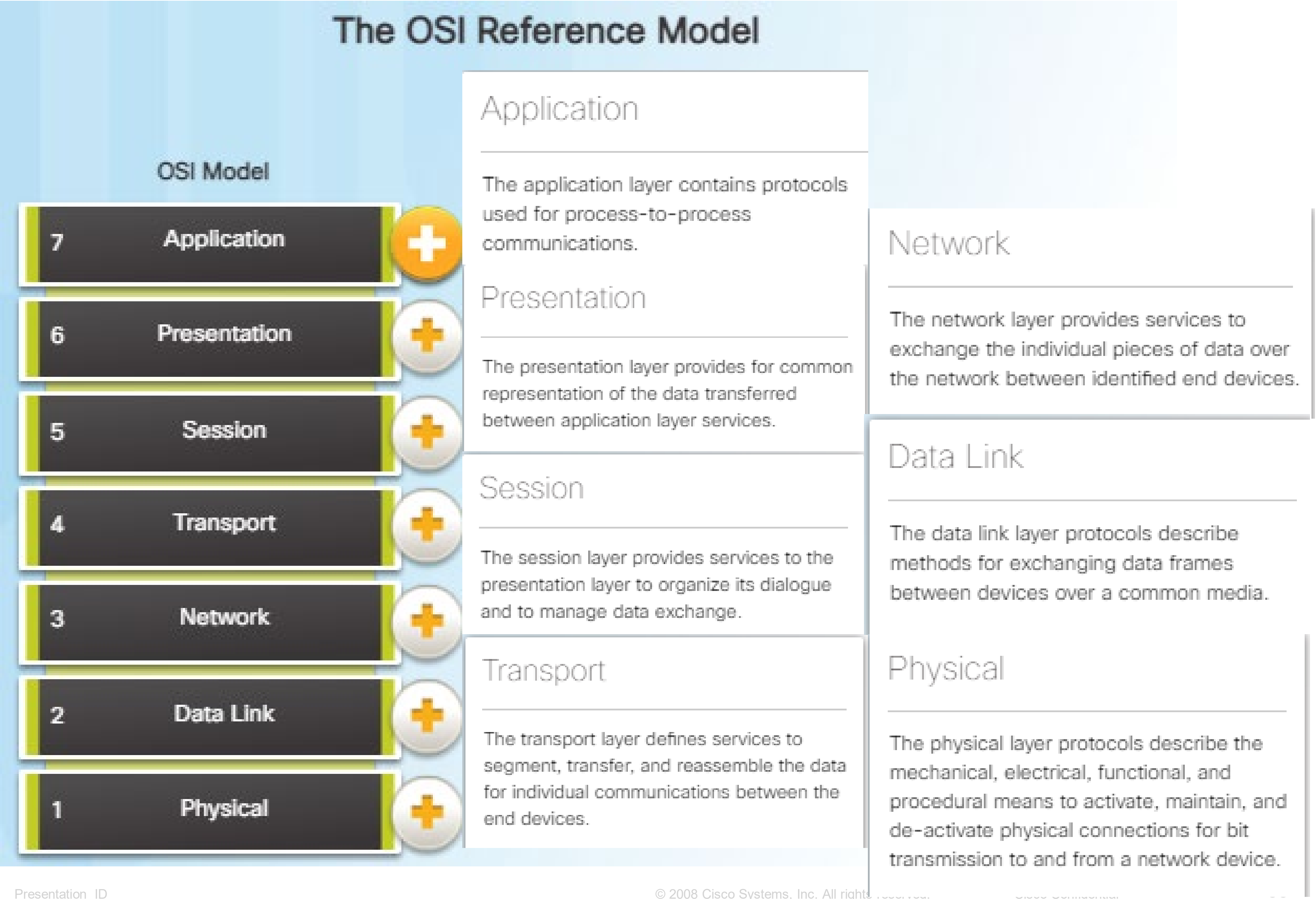
	OSI Model	TCP/IP Model
7	Application	Application
6	Presentation	
5	Session	
4	Transport	Transport
3	Network	Internet
2	Data Link	Network Access
1	Physical	

The key similarities are in the transport and network layers; however, the two models differ in how they relate to the layers above and below each layer.



TCP/IP Model

Application	Represents data to the user, plus encoding and dialog control.
Transport	Supports communication between various devices across diverse networks.
Internet	Determines the best path through the network.
Network Access	Controls the hardware devices and media that make up the network.



The OSI Reference Model

OSI Model

Application

The application layer contains protocols used for process-to-process communications.

Presentation

The presentation layer provides for common representation of the data transferred between application layer services.

Session

The session layer provides services to the presentation layer to organize its dialogue and to manage data exchange.

Transport

The transport layer defines services to segment, transfer, and reassemble the data for individual communications between the end devices.

Network

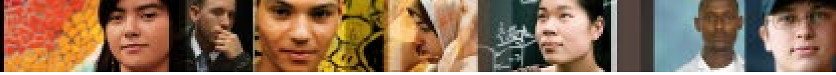
The network layer provides services to exchange the individual pieces of data over the network between identified end devices.

Data Link

The data link layer protocols describe methods for exchanging data frames between devices over a common media.

Physical

The physical layer protocols describe the mechanical, electrical, functional, and procedural means to activate, maintain, and de-activate physical connections for bit transmission to and from a network device.



What are Connections?

Models of Communication (Cont.)

- Simplified IoT Architecture
  - Developing IoT systems to interconnect smart objects is a complex task. Many smart objects designed by different vendors have constraints concerning proprietary software that makes interoperability a challenge. Also, devices such as sensors, actuators, and controllers, have constraints in bandwidth, power, size, and installed location. These constraints amplify the issues surrounding security and privacy.
  - Several architectures exist to help facilitate the design and creation of IoT systems. The OSI model, TCP/IP model, and the IoT World Forum Reference model have been presented as examples.
  - Emerging opinions are now opting for a simpler approach based on the type or level of connections between the smart objects. Each level of expanded connectivity has a different set of design issues and requirements for security and privacy to consider.
    - A simpler approach is based on connection levels. The levels are:
      - Device-to-Device
      - Device-to-Cloud
      - Device-to-Gateway-to-Cloud
      - Device-to-Gateway-to-Cloud-to-Application

What are Connections?

Models of Communication (Cont.)

- **Device-to-Device** (Figure 1)
- IoT solutions often support one smart object connecting directly to another via a wireless protocol such as Bluetooth or Zigbee. An example of this level is a sensor that is located in a vineyard and detects dry soil. It sends a signal to an actuator that triggers the watering system.

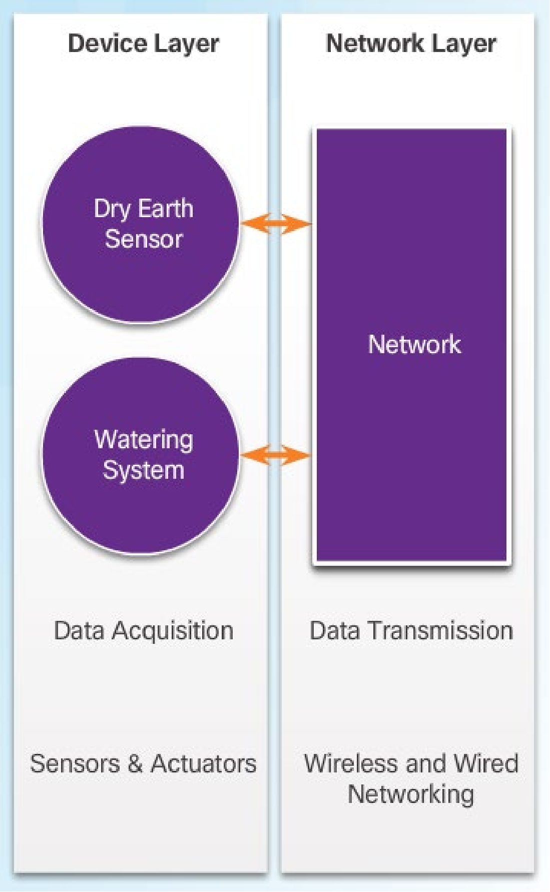


Figure 1

- **Device-to-Cloud (Figure 2)**
- In a device-to-network-to-cloud communication model, the IoT device connects through a local network directly to an Internet cloud service using traditional wired Ethernet or Wi-Fi connections. This model establishes a connection between the device, the IP network, and the cloud to allow the exchange of data and control messages.

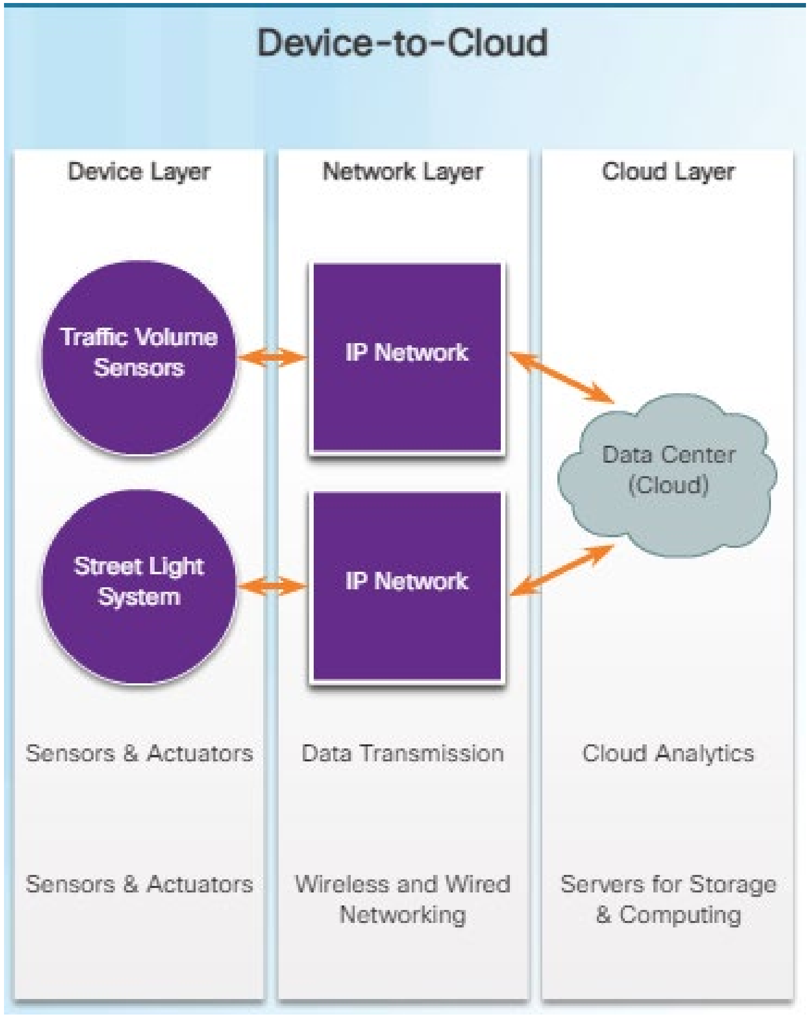


Figure 2

- **Device-to-Gateway-to-Cloud (Figure 3)**
- Many smart devices, such as fitness trackers, are not IP-enabled and do not have the native ability to connect directly to the fog or the cloud. For these devices, there is application software operating on a local gateway device which acts as an intermediary between the device and the cloud service. The gateway may also provide security and data or protocol translation. For devices, like fitness trackers, the gateway is often an application running on a smartphone.

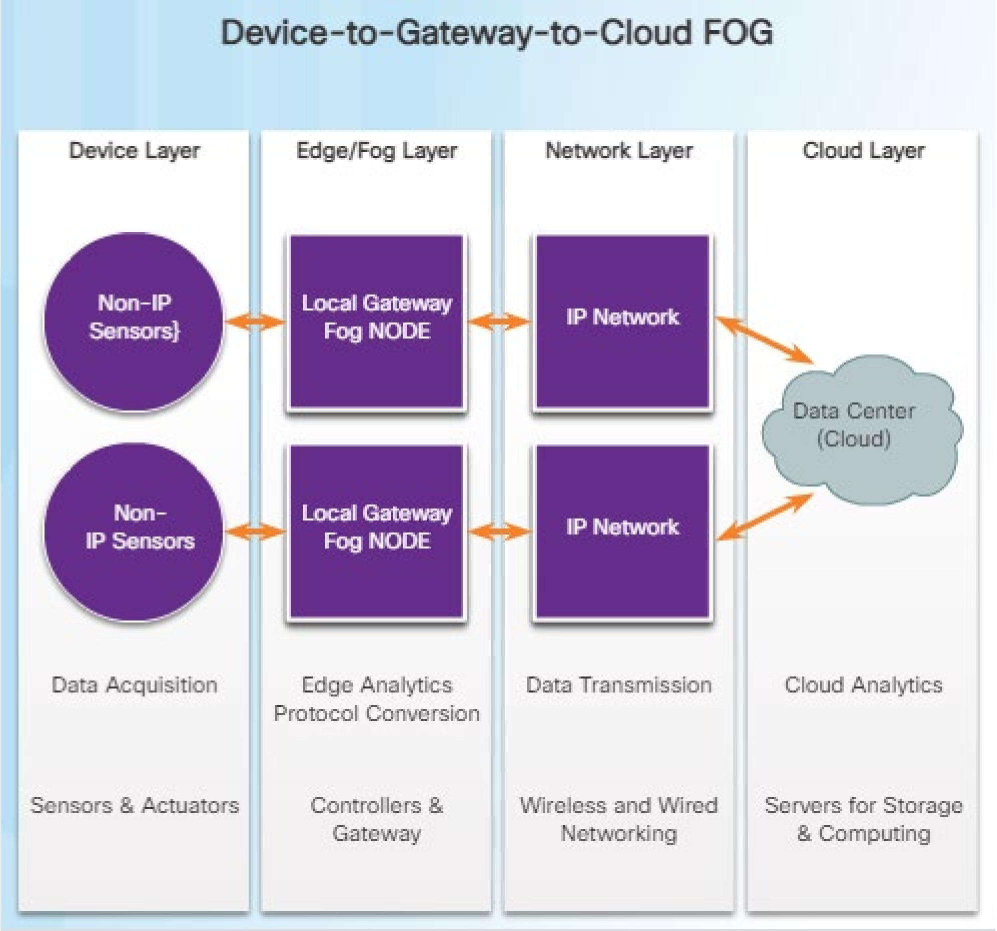


Figure 3

- **Device-to-Gateway-to-Cloud-to-Application (Figure 4)**
- Another connection option supports smart device data collection and transfer through a gateway to a local IP network. The data then flows to the fog or the cloud and is then available for users to export and analyze. The data is often analyzed in combination with data from other sources or other cloud services.
- Knowledge of the four basic levels of connections will ensure that consideration is given to device interoperability and open standards. These are key considerations when developing an internetworked IoT system.

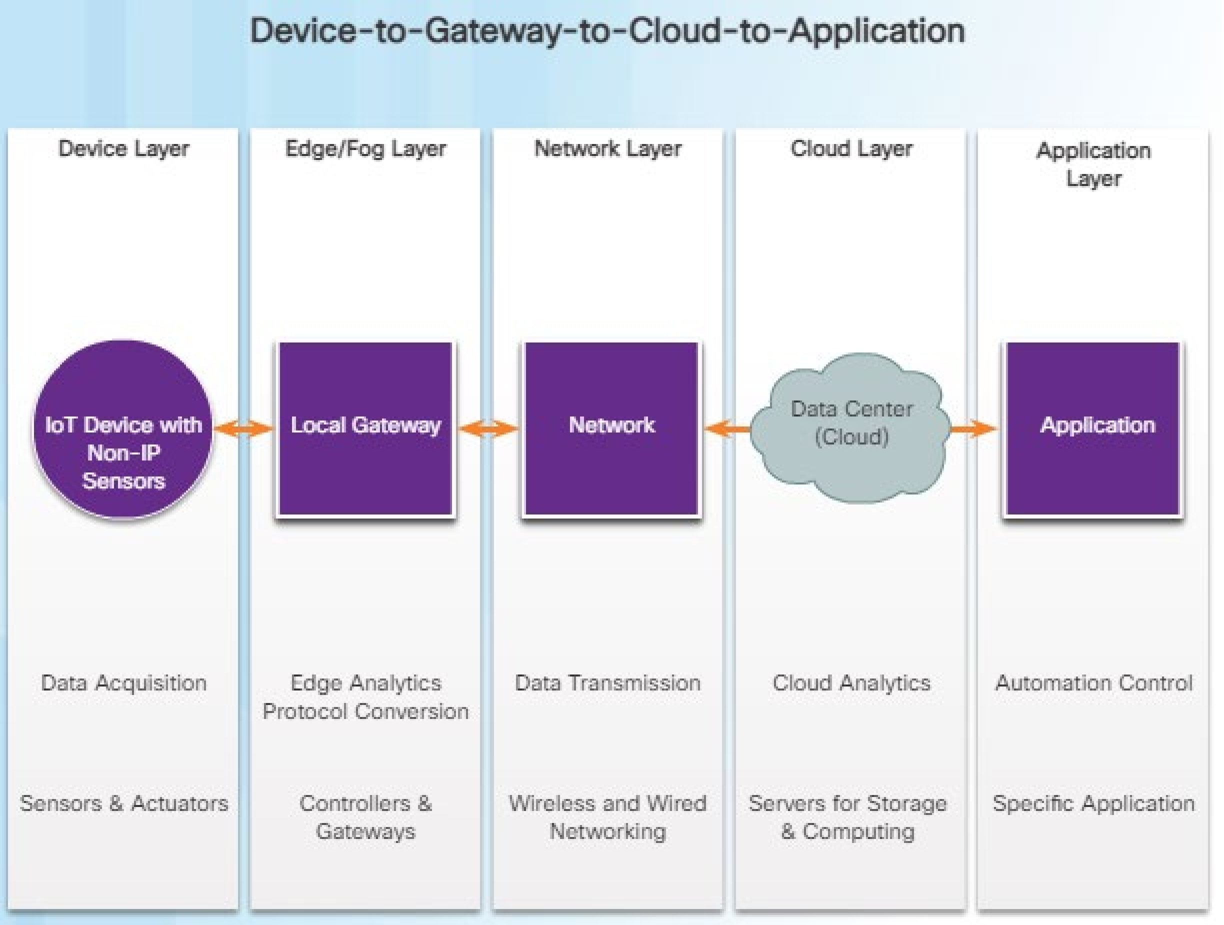


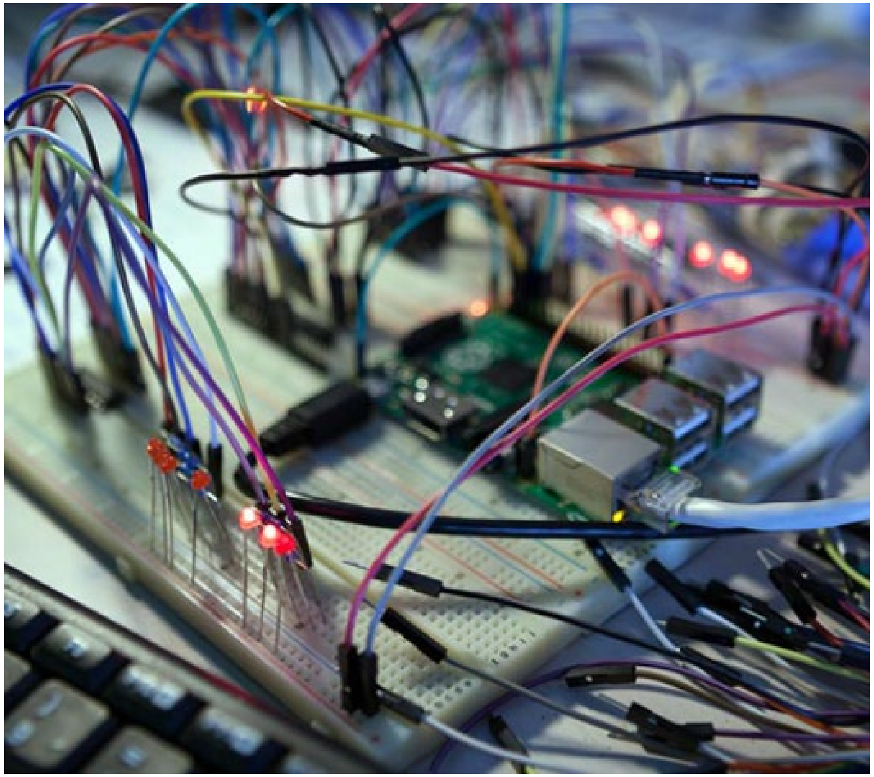
Figure 4

What are Connections?

1.2.2 Layers of Connections

- Connections Within Networks
  - Connections can have different contexts.
  - Power connections, circuit connections or network connections.
- There are multiple, complementary meanings of the word “connection" when designing, configuring, or troubleshooting IoT systems.
- First, devices must typically be “connected” to some source of power. Types of connections for power include batteries, direct connections to AC power, external power supplies (to convert AC to DC), and Power over Ethernet (PoE). Most devices connect to the local power grid as provided by a wall outlet. However, IoT devices are also used in remote locations where access to power is often limited or unavailable. In these situations energy harvesting is done from light (solar cells), vibration (pressure piezoelectric elements) or temperature difference (thermocouple) to power the devices.

Raspberry Pi Connected to Breadboard

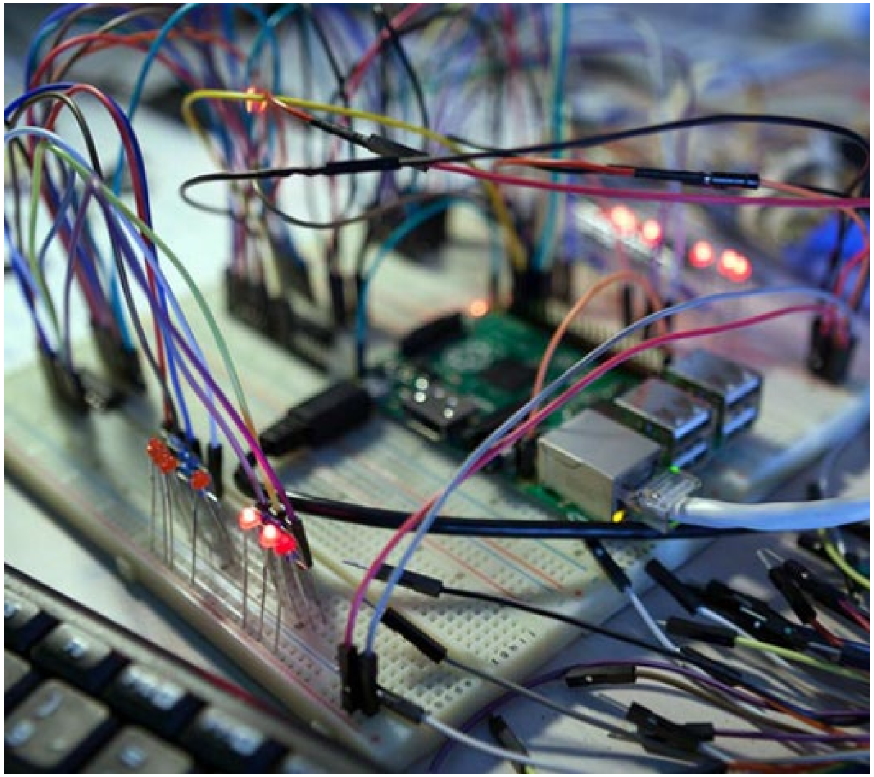


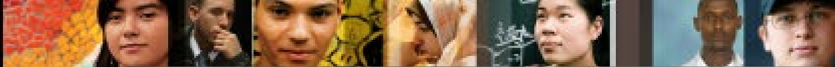
What are Connections?

1.2.2 Layers of Connections

- A second meaning of the word “connection” relates to the wires and circuitry used in IoT devices. All IoT devices have circuitry interconnecting their sensors, actuators, and controllers together. To simplify this process when prototyping new devices, a solderless breadboard is often used. A breadboard provides a flexible way to make electronic circuit-level connections to all types of components. For example, in the figure a Raspberry Pi is connected to a breadboard providing access to LEDs, resistors, and integrated circuits.
- A third meaning of the word “connection” relates to the OSI Layer 2 and Layer 3 networking links. This is the most important meaning when referring to the IoT devices. The following pages describe the media, protocols, and standards required to achieve successful network connections.

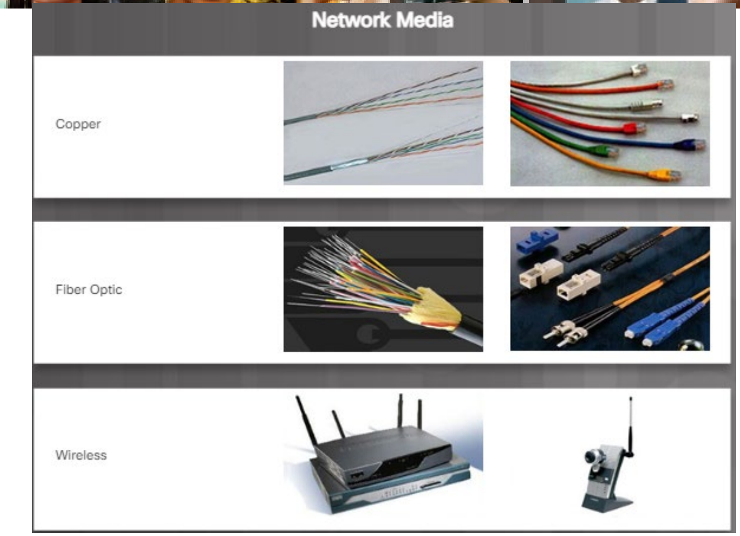
Raspberry Pi Connected to Breadboard





What are Connections?

1.2.2 Layers of Connections

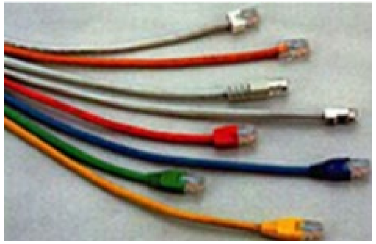


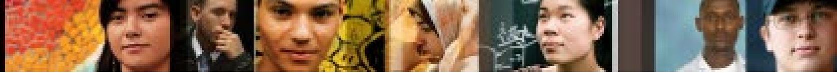
- Physical Connections
  - Relate to the media and cable type.
  - Common media types include copper, fiber optics and wireless.
- There are three types of media used by IoT devices to communicate:
- **Copper** - Networks use copper media because it is inexpensive, easy to install, and has low resistance to electrical current. However, copper media is limited by distance and signal interference. Therefore, all copper media must follow strict distance limitations as specified by the guiding standards.
- **Fiber optics** – Fiber-optic cables can travel significantly longer distances than copper cables due to their immunity to signal interference. The sending device transmits the binary bits as light pulses using LEDs or lasers. The receiving device uses photodiodes to detect the light pulses and convert them to voltages. Fiber-optic cables are broadly classified as single-mode fiber (SMF) and multimode fiber (MMF). SMF consists of a very small core using expensive laser technology to send a single ray of light over long distances spanning hundreds of kilometers. MMF consists of a larger core and uses lower-cost LED emitters to send light pulses. MMF is popular in LAN deployments because it can support 10 Gb/s over 550 meters links.
- **Wireless** – Wireless consists of a wide range of connection options including electromagnetic signals, radio and microwave frequencies, and satellite links.
- All copper and fiber cable connectors adhere to specific physical layer standards. These standards specify the mechanical dimensions of the connectors and the acceptable electrical properties of each type. These network media also commonly use modular jacks and plugs to provide easy connection and disconnection.

What are Connections?

Layers of Connections (cont'd)

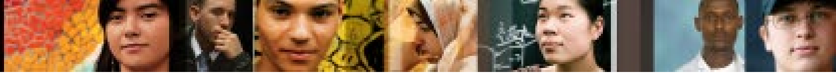
- Data Link and Network Connections
  - Network communication requires protocols to establish the rules of communications. Data Link protocols:
    - Allow the upper layers to access the media
    - Prepare network data for the physical network
    - Control how data is placed and received on the media
    - Exchange frames between nodes over a physical network media, such as copper or fiber-optic
    - Receive and directing packets to an upper layer protocol
    - Perform error detection
  - The most popular data link layer connection used in wired networks is Ethernet.
  - Other data link protocols include wireless standards such as IEEE 802.11 (Wi-Fi), IEEE 802.15 (Bluetooth), and cellular 3G or 4G networks.
  - LoRaWAN and NB-IoT are examples of emerging IoT supporting technologies.





Data Link and Network Connections

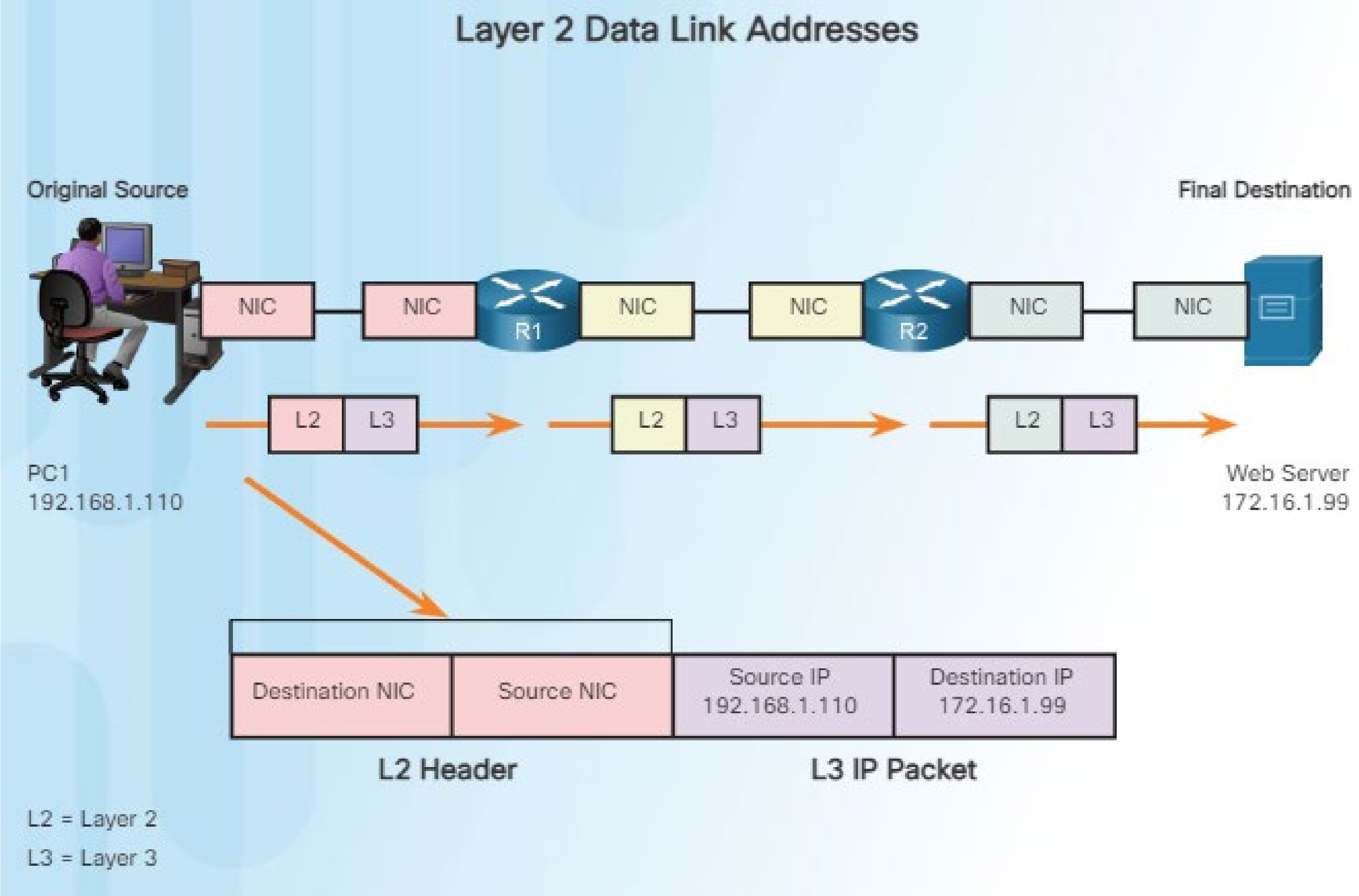
- When delivering power to components, all devices adhere to strict standards as specified by governmental agencies. Protocols are not required to successfully supply power. For instance, you simply plug in the component to a wall outlet and the device is powered.
- Network communication on the other hand, requires the use of protocols to establish the rules of communications. Messages can only be successfully exchanged between devices using commonly agreed on protocols.
- The most popular data link layer (Layer 2) connection used in wired networks is Ethernet. Ethernet is a Layer 2 protocol which delivers frames between devices on a LAN. Other commonly used data link protocols include wireless standards such as IEEE 802.11 (Wi-Fi), IEEE 802.15 (Bluetooth), and cellular 3G or 4G networks.
- Several newer technologies are emerging to support the connectivity of “things” in the IoT, such as:
- **LoRaWAN** – a low power wide-area network
- **Narrowband IoT (NB-IoT)** – a new way of communicating with “things” that require small amounts of data, over long periods, in hard to reach places
- **Time Sensitive Networks** – enhanced Ethernet that supports latency-sensitive applications that require deterministic network performance



Data Link and Network Connections

- Data link layer protocols are responsible for several activities:
- Allowing the upper layers to access the media
- Accepting Layer 3 packets and encapsulating them into frames
- Preparing network data for the physical network
- Controlling how data is placed and received on the media
- Exchanging frames between nodes over a physical network media, such as copper or fiber-optic
- Receiving and directing packets to an upper layer protocol
- Performing error detection
- Layer 3 protocols are responsible for providing addressing to reach remote networks. The most common network layer (Layer 3) protocol used in network connections and on the Internet is the IP protocol.
- In the next figure, the user at PC1 is sending a file to the Web server on a different network. It is important to note that all devices on the network had to agree to use Ethernet and IPv4 for network communications to be possible.

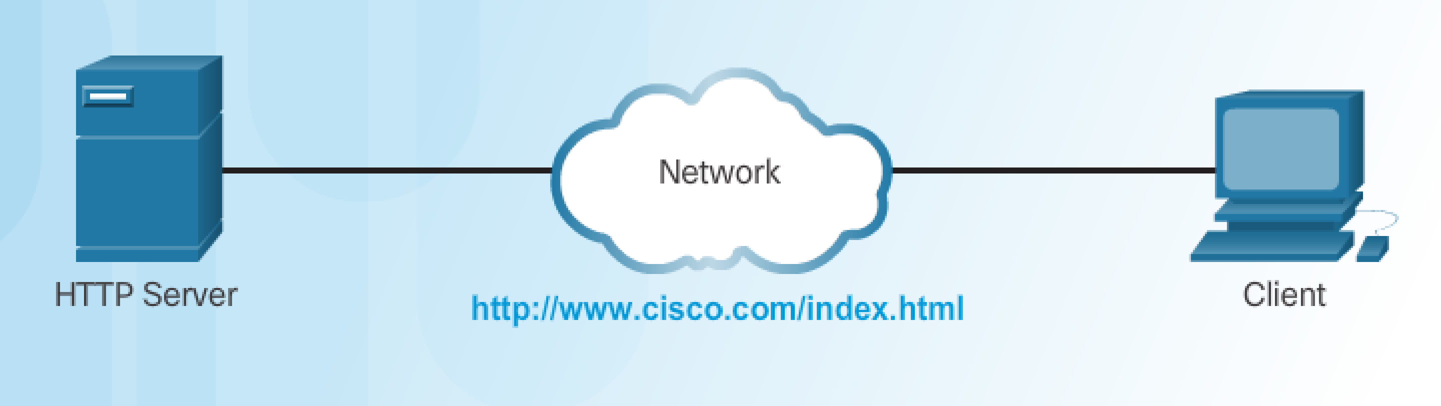
Data Link and Network Connections

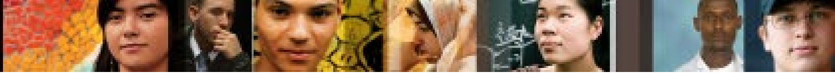


What are Connections?

Layers of Connections (Cont.)

- Application Connections
  - The IoT supports many types of connections.
  - Devices must use the same application layer protocols to connect.
  - The application will vary depending on the devices and type of connection involved.
  - MQTT and REST are newer application protocols, created to support IoT devices that connect in the myriad of different types of remote configurations.
  - MQTT is a lightweight messaging protocol with minimal overhead that provides high data integrity and security for remote environments.
  - REST or RESTful web services is a type of API designed to make it easier for programs to interact over the Internet.

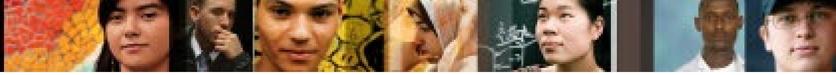




- The IoT supports many types of connections: machine to machine (M2M), machine to gateway (M2G), and machine to the cloud (M2C). Devices must use the same application layer protocols to connect. The application will vary depending on the devices and type of connection involved.
- Figure 1 represents a well-known example of a client that will use the HTTP protocol to communicate with the Web Server. The web server is configured and managed to allow people to interact with a web page.
- Newer application layer protocols, such as MQTT and REST, have emerged to support IoT devices that connect in the myriad of different types of remote configurations.
- Message Queuing Telemetry Transport (MQTT) is a lightweight messaging protocol with minimal overhead that provides high data integrity and security for remote environments.
- Representational State Transfer (REST), or RESTful web services, is a type of API designed to make it easier for programs to interact over the Internet. REST allows for the use of the HTTP protocol and URLs to request web services.
- Both of these protocols will be covered in more detail in later chapters.

1.2.3 Impact of Connections on Privacy and Security

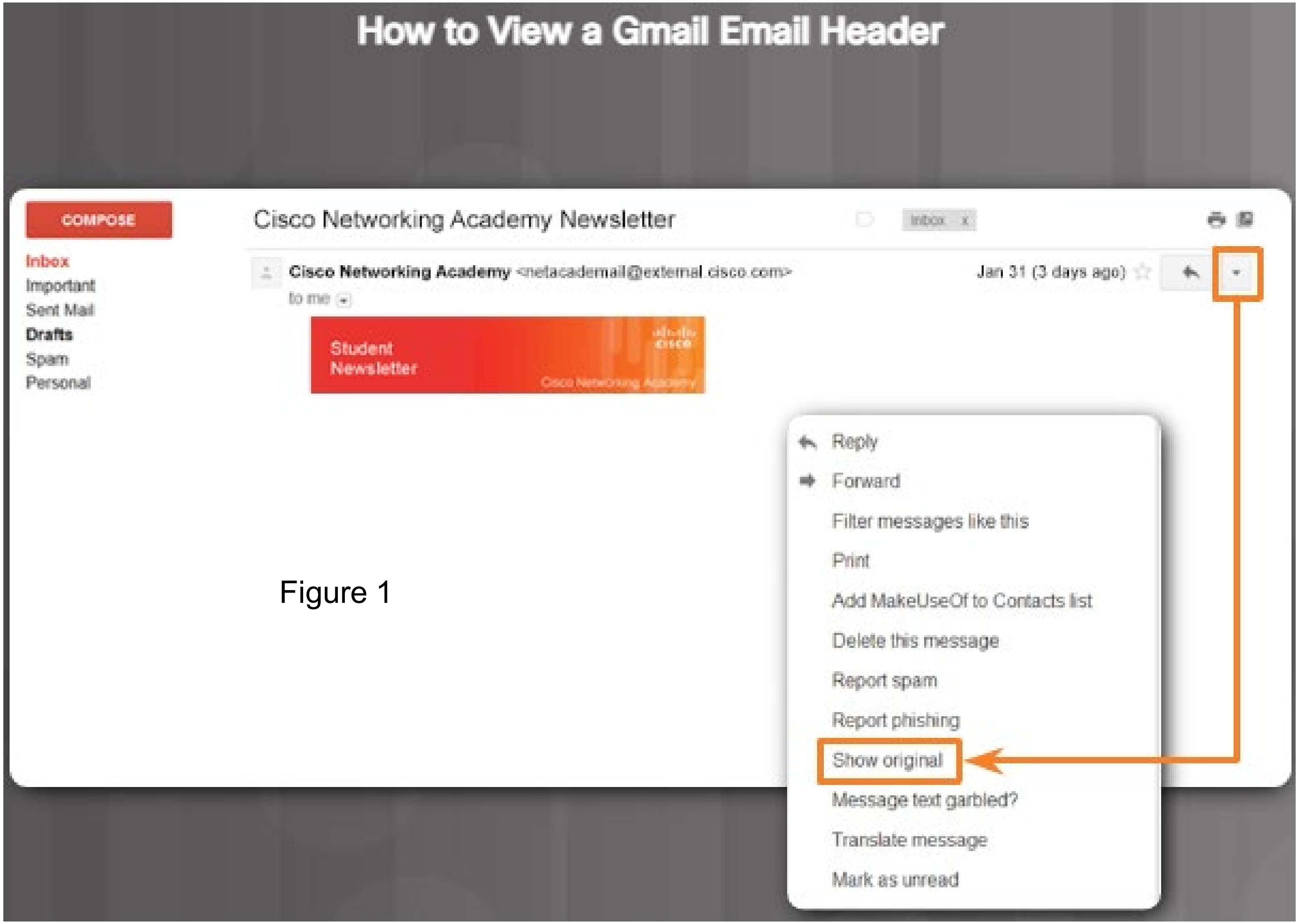
- What is Metadata?
  - Metadata refers to the data about data.
  - Metadata can be embedded within a digital object or it can be stored separately.
  - Metadata is not usually seen by a user.
- The Impact of IoT on Privacy
  - Suggestions and design considerations concerning privacy include:
    - Transparency
    - Data Collection and Use
    - Data Access
- Challenges for Securing IoT Devices
  - Some IoT network security impacting factors include:
    - Increasing Number of Devices
    - Non-Traditional Location of Devices
    - Changing Type and Quantity of Gathered Data
    - Lack of Upgradeability



What is Metadata?

- The term “metadata” means data about data. Metadata can be embedded within a digital object or it can be stored separately. Metadata is not usually seen by a user. As an example, an email header contains information at the beginning that represents the path an email took to get to you, the name and IP information of who the email is going to, the name and IP information of the person who sent the email, and the time and date that the email was sent. This information is considered metadata. Metadata can contain both personal information and descriptive or administrative information. A digital photograph might contain the time and GPS location of where the photo was taken. It might also contain exposure settings and information about the camera model.
- Metadata can be collected, stored, and analyzed for good purposes by organizations such as governments, marketing organizations, and healthcare providers. The data could be useful to support government initiatives, emerging shopping trends, or to improve access to doctors and walk-in clinics. Metadata can also be used for storing and archiving data. Unfortunately the information in metadata can also be exploited and used to invade our privacy, track our movements, or possibly steal our money or identity.
- In some applications, metadata can be turned off. This is frequently found under the **Settings** or **Options** tab. Because each application is different, check the documentation to see if it is possible.
- Figure 1 shows how to view a Gmail header and Figure 2 shows an example of metadata preceding an email.

What is Metadata?



How to View a Gmail Email Header

Cisco Networking Academy Newsletter

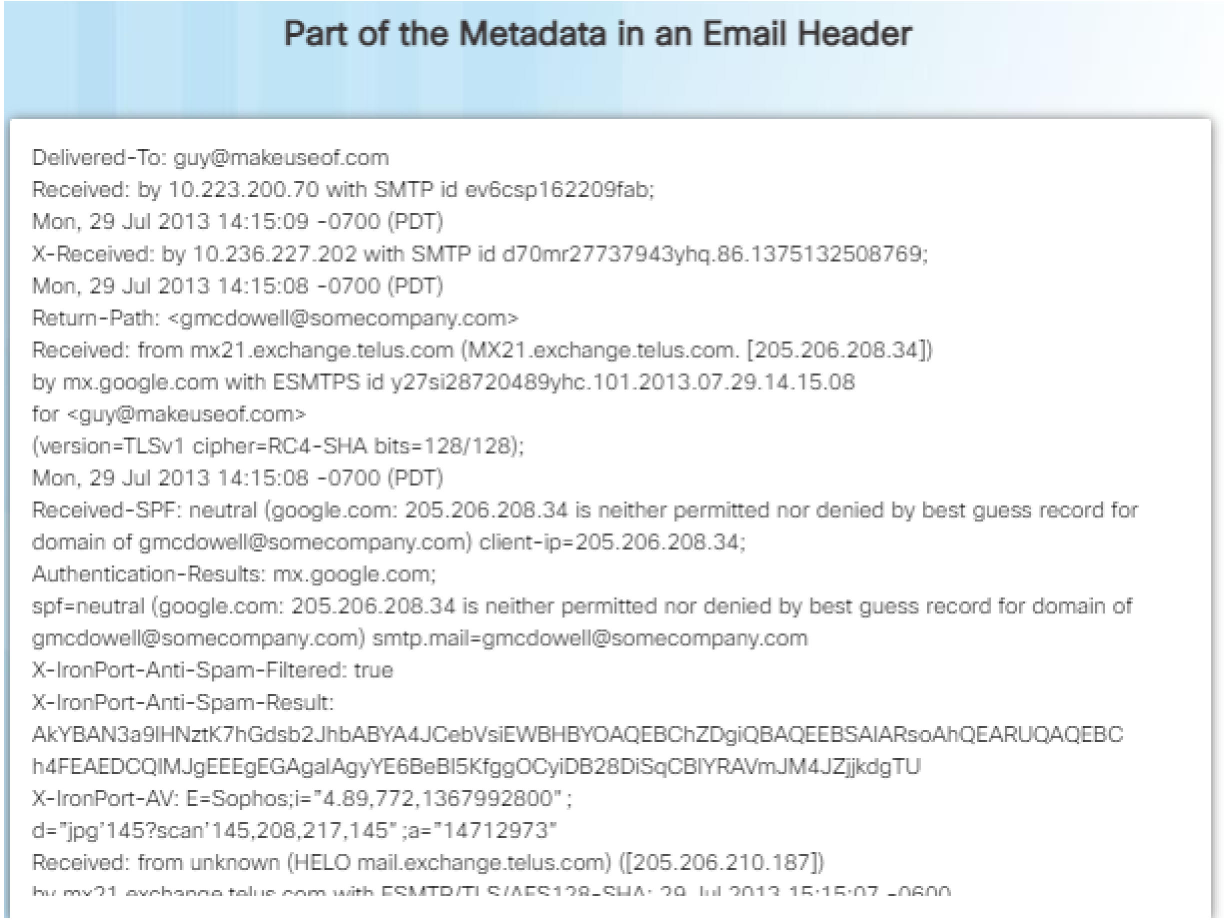
Cisco Networking Academy <netacademail@external.cisco.com>

to me

Jan 31 (3 days ago)

Figure 1

What is Metadata?



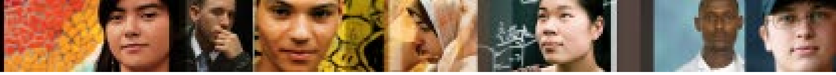
Part of the Metadata in an Email Header

```
Delivered-To: guy@makeuseof.com
Received: by 10.223.200.70 with SMTP id ev6csp162209fab;
Mon, 29 Jul 2013 14:15:09 -0700 (PDT)
X-Received: by 10.236.227.202 with SMTP id d70mr27737943yhq.86.1375132508769;
Mon, 29 Jul 2013 14:15:08 -0700 (PDT)
Return-Path: <gmcdowell@somecompany.com>
Received: from mx21.exchange.telus.com (MX21.exchange.telus.com. [205.206.208.34])
by mx.google.com with ESMTPS id y27si28720489yhc.101.2013.07.29.14.15.08
for <guy@makeuseof.com>
(version=TLSv1 cipher=RC4-SHA bits=128/128);
Mon, 29 Jul 2013 14:15:08 -0700 (PDT)
Received-SPF: neutral (google.com: 205.206.208.34 is neither permitted nor denied by best guess record for
domain of gmcdowell@somecompany.com) client-ip=205.206.208.34;
Authentication-Results: mx.google.com;
spf=neutral (google.com: 205.206.208.34 is neither permitted nor denied by best guess record for domain of
gmcdowell@somecompany.com) smtp.mail=gmcdowell@somecompany.com
X-IronPort-Anti-Spam-Filtered: true
X-IronPort-Anti-Spam-Result:
AkYBAN3a9IHNztK7hGdsb2JhbABYA4JCebVsiEWBHBYOAQEBChZDgiQBAQEEBSAIARsoAhQEARUQAQEBC
h4FEAEDCQIMJgEEEgEGAgaIAgyYE6BeBI5KfggOCyiDB28DiSqCBIYRAVmJM4JZjjkdgTU
X-IronPort-AV: E=Sophos;i="4.89,772,1367992800" ;
d="jpg'145?scan'145,208,217,145" ;a="14712973"
Received: from unknown (HELO mail.exchange.telus.com) ([205.206.210.187])
by mx21.exchange.telus.com with ESMTP/TLS/AES128-SHA; 29 Jul 2013 15:15:07 -0600
```

Figure 2

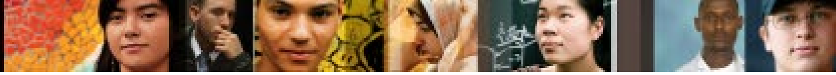
The Impact of the IoT on Privacy

- Many IoT systems are designed to monitor and regulate people and our physical environments. These IoT systems and devices can enable the creation of vast amounts of metadata. People must be able to trust that any of their personally identifiable information (PII) that is collected is secure and private. PII is any information that can identify, contact, or locate an individual. PII can also be combined from different sources to identify elements of an individual’s traits or lifestyle. In order to protect individuals and instill trust, new IoT systems should be designed with security and privacy in mind from the beginning.



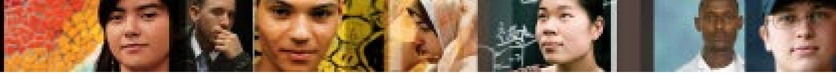
The Impact of the IoT on Privacy

- **Suggestions and design considerations concerning privacy:**
- **Transparency** - People should know what types of personal data are being collected, why the data is being collected, and where it is to be stored. This transparency of data collection and processing will alleviate concern and avoid unpleasant circumstances for owners and users of smart objects.
- **Data Collection and Use** - Smart devices should only store personal data that is adequate and relevant in relation to the purpose for which they are collected. Data that hides the identity of the person should be used wherever possible.
- **Data Access** - Before new systems are deployed, designers should determine who is able to access personal data collected by smart objects and under which conditions. If appropriate and clear procedures are established and promoted, people affected by the devices can make their own judgement about using the system.
- To cover issues of privacy, software, hardware, and service, vendors ask us to read and approve Terms of Service and Agreement documents. We all tend to check them as read, because they are so long and full of “legalese”. The next time you install new software or hardware, we suggest that you take the time to read the Terms of Service from the perspective of the privacy and security of your personal data. You might find it interesting.



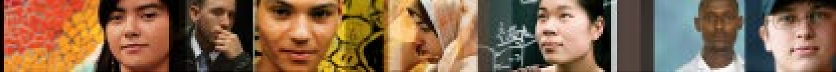
Challenges for Securing IoT Devices

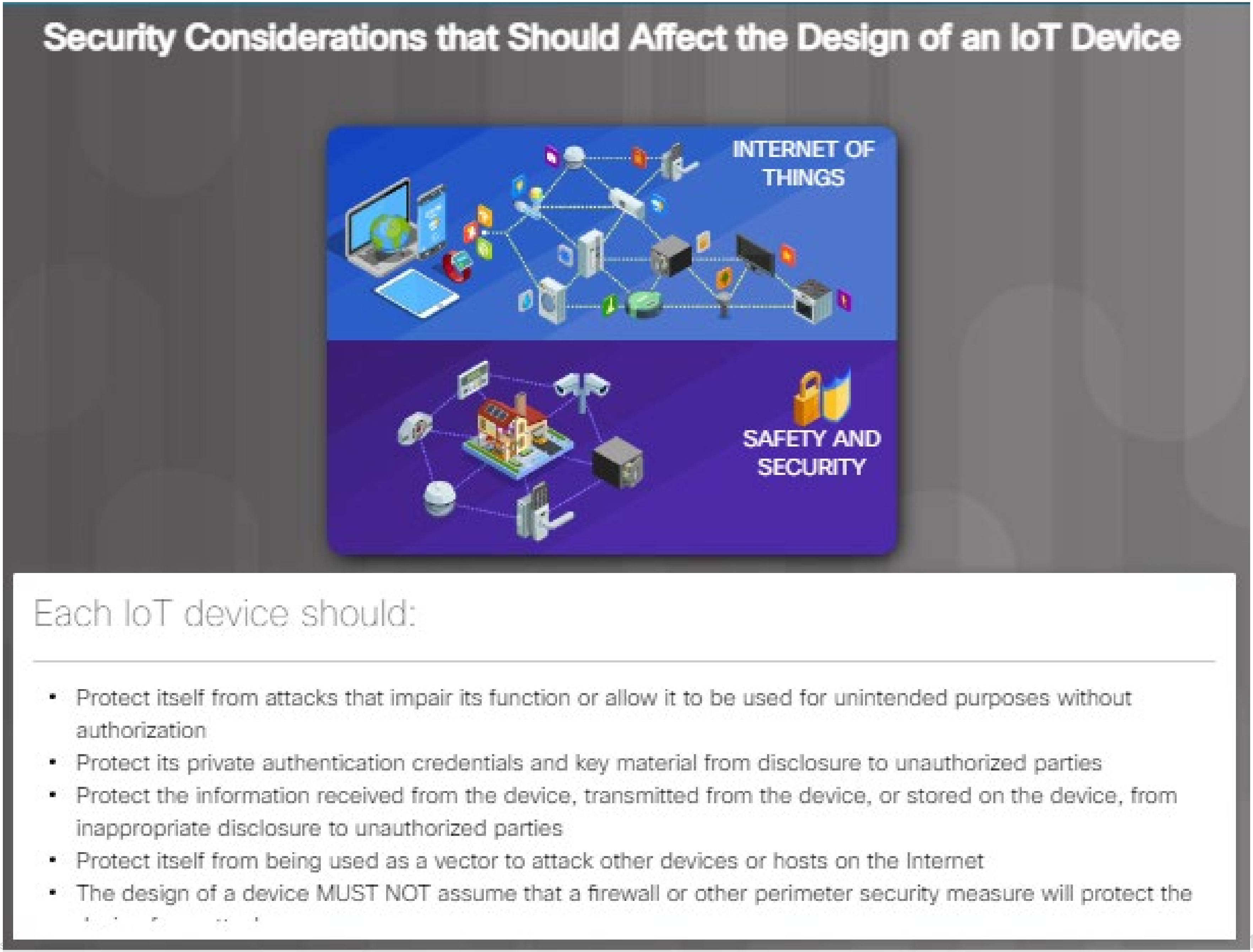
- Innovations and emerging technologies in the IoT space are having an impact on our daily lives. We can better sense our physical environment, track an individual's physical fitness, monitor embedded medical devices, make processing more efficient, and ease traffic and parking congestion in real-time. To keep pace with technology and competitors, IoT devices are developed with the necessary network connectivity capabilities but often do not implement strong network security. Network security is a critical factor when deploying IoT devices. Here are some factors that impact network security in the IoT:
- **Increasing Number of Devices** - The number of interconnected sensors and smart devices is growing exponentially, increasing the opportunity for attacks. Sensors and smart devices tend to be small devices, with varying operating systems, CPU types, and memory. Many of these entities are expected to be inexpensive, single-function devices with rudimentary network connectivity. Consider a homeowner purchasing a home security and monitoring system. This system is designed to track the temperature and brightness in each room, and the frequency and time of the door opening and closing. This data can be stored locally in the homeowner’s computer but is most likely uploaded and stored on the vendor’s system or in the cloud. Soon all of the neighbors decide to use the same system. Use of this system then expands throughout the city. This results in a growing number of sensors and exponentially more gathered data. Methods must be taken to ensure the authenticity, integrity, and security of the data, the path from the sensor to the collector, and the connectivity to the device.
- **Non-Traditional Location of Devices** - Some connected IoT devices are able to interact with the physical world. They are now located in appliances, in automobiles, on or in our bodies, and in our homes. Sensors may gather data from the refrigerator or the heating system. They could also be located in city lampposts or attached to tree trunks. These non-traditional locations make physical security difficult or impossible to achieve. Attackers may have direct physical access to IoT devices. Given the highly interconnected nature of IoT devices, this can create a situation where a weak link in a small sensor or actuator could jeopardize security locally or globally.



Challenges for Securing IoT Devices

- **Changing Type and Quantity of Gathered Data** - IoT sensor-enabled devices are collecting more and more data of a personal nature. Wearable fitness trackers, home monitoring systems, security cameras, debit card transactions are all collecting personal data as well as environmental data. Data is often combined from different sources and users are unaware of this situation. Combining fitness monitoring data with house monitoring data could produce data points to help map the movements or location of a homeowner. This changing type of data collection and aggregation can be used for good purposes to help the environment. It also increases the possibility of invasion of our privacy, identity theft, and corporate espionage.
- **Lack of Upgradeability** - IoT sensor-enabled devices may be located in remote and/or inaccessible locations where human intervention or configuration is almost impossible. These devices may also contain fairly basic technology designed for one simple task. The devices are often designed to be in service many years longer than is typical for conventional high-tech equipment. It is possible that these devices could outlive the company that created them. This creates the possibility of having installed devices with no means of long-term support. Some IoT devices are intentionally designed without the ability to be upgraded, or they might be deployed in situations that make it difficult or impossible to reconfigure or upgrade. New vulnerabilities are uncovered all of the time. If a device is non-upgradeable, then the vulnerability will exist for the rest of its lifetime. If a device is upgradeable, manufacturing companies need to understand that the typical consumer may not have a technology background, therefore, the upgrade process should perform automatically or be easy enough to be performed by a layperson.
- Before deploying a new IoT system, security measures must be designed to address as many of the security vulnerabilities as possible. Minimally, standardized data security measures should be in place to prevent unlawful access, alteration, or loss of smart object data. Strong encryption and authentication frameworks should be used to limit the risk of the vulnerabilities.
- The figure outlines security considerations that should affect the design of an IoT device as proposed by the IETF.





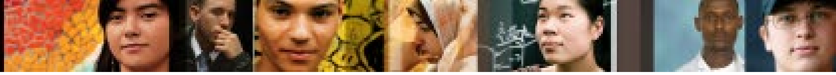
Security Considerations that Should Affect the Design of an IoT Device

Each IoT device should:

- Protect itself from attacks that impair its function or allow it to be used for unintended purposes without authorization
- Protect its private authentication credentials and key material from disclosure to unauthorized parties
- Protect the information received from the device, transmitted from the device, or stored on the device, from inappropriate disclosure to unauthorized parties
- Protect itself from being used as a vector to attack other devices or hosts on the Internet
- The design of a device MUST NOT assume that a firewall or other perimeter security measure will protect the

1.3 Chapter Summary

Cisco | Networking Academy®
Mind Wide Open™



Chapter Summary

Summary

- The Internet of Things (IoT) is all around us. An IoT system is usually made up of sensors to monitor events, actuators to influence the environment, hardware to create the platform and its connections, and software to provide a framework to execute processes.
- A process is a series of steps or actions taken to achieve a desired result.
- Layered networking models are used to illustrate and model how devices communicate. Physical, data link, and network layers are concepts that are used to illustrate how network communication operates.
- Security and privacy issues must be considered in all phases of creation of an IoT system. Each level of connectivity brings with it different requirements and concerns..

Cisco | Networking Academy®

Mind Wide Open™