Année académique 2022 - 2023

HEH be
Sciences et technologies

Avenue V. Maistriau 8a
B-7000 Mons
+32 (0)65 33 81 54
tech-mons@heh.be

WWW.HEH.BE

UE : Fonctionnement des systèmes 1

Bachelier en Informatique & systèmes orientation réseaux et télécommunications

Internet of everything

Erwin DESMET – erwin.desmet@heh.be

Formations de Bacheliers et de Masters organisées par la Fédération Wallonie-Bruxelles

FÉDÉRATION WALLONIE-BRUXELLES

pôle hainuyer

Content

1. What is the Internet of Things?

1.1 Internet of Things

1.1.1 The Internet

1.1.1.1. Here's to Humanity

The Internet has evolved in ways that we could never have imagined. In the beginning, advancements occurred slowly. Today, innovation and communication are happening at a remarkable rate.
From its humble beginning as the Advanced Research Projects Agency Network (ARPANET) in 1969, when it interconnected a few sites, it is now predicted that the Internet will interconnect 50 billion things by 2020. The Internet now provides global connections that make web surfing, social media, and smart mobile devices possible.
Watch how the Internet emerged over the last 25 years and see a glimpse into the future in the PwP! (video 1)

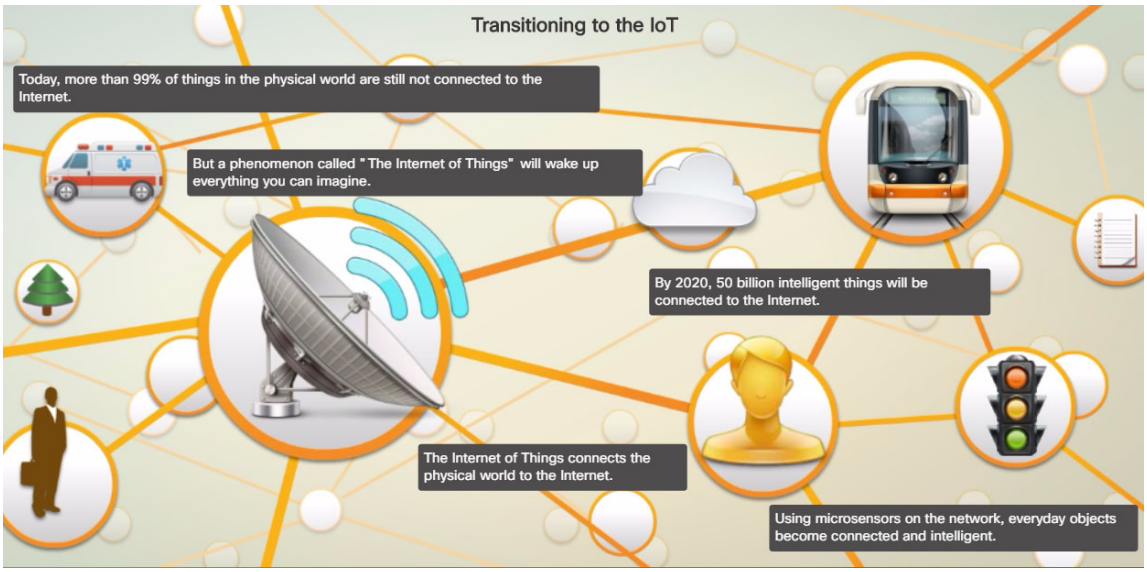
1.1.1.2. The Internet : The Place to Go

Normally, when people use the term Internet, they are not referring to the physical connections in the real world. Rather, they tend to think of it as a formless collection of connections. It is the "place" people go to find or share information. It is the 21st century library, video store, and personal photo album.

1.1.1.3. Internet Maps

In actuality, the Internet is essentially a network of networks.
Each of us connects to the Internet using a physical cable or through wireless media. Underneath this network of networks lies a very real backbone of connections that bring the world to our personal computing devices.
The figure is an oversimplified map of global Internet traffic; however, it depicts how countries and continents are connected. Click http://www.submarinecablemap.com/ that depicts the location of submarine cables.
After you have opened the telegeography map, click any cable on the map to highlight that cable and see the points at which it connects with land. (Alternatively, you can select any cable from the list to the right of the map.)
Click any city on the map to see a list of all the cables that connect to that city.
A great amount of engineering, effort, and money goes into the planning and deployment of each of these cables.

1.1.1.4. Transitioning to the IoT



1.1.1.6. The Circle Story

In a very short time, the Internet has dramatically changed how we work, live, play, and learn. Yet, we have barely scratched the surface. Using existing and new technologies, we are connecting the physical world to the Internet. It is by connecting the unconnected that we transition from the Internet to the Internet of Things.
Click play (video 2) to see Cisco's vision of how the Internet of Everything could impact your everyday life.

2. Everything is Connected

2.1. Digital Transformation

2.1.1. Digitalization Transform Business

2.1.1.1. The Evolution of Digital Transformation

Tell the truth …. how many of you could actually make it through a day without your smartphone?
In our world today, there are more smart devices than there are people. A growing number of people are connected to the Internet, in one way or another, 24 hours a day. An ever-increasing number of people have, and rely on, three, four, or more smart devices. These might include smartphones, exercise and health monitors, e-readers, and tablets. As shown in Figure 1, by 2020, it is forecast that each consumer will have an average of 6.58 smart devices.

How is it possible for so many devices to be connected?

Modern digital networks make all of this possible. The world is quickly being covered with networks that allow digital devices to interconnect and transmit. Think of the mesh of networks like a digital skin surrounding the planet, as illustrated in Figure 2. With this digital skin, mobile devices, electronic sensors, electronic measuring devices, medical devices, and gauges are all able to connect. They monitor, communicate, evaluate, and in some cases automatically adjust to the data that is being collected and transmitted.

As society embraces these digital devices, as digital networks continue to grow around the world, and as the economic benefits of digitization continue to grow, we are seeing a digital transformation. Digital transformation is the application of digital technology to provide the stage for business and industry to innovate. This digital innovation is now being applied to every aspect of human society.

2.1.1.2. The Impact of Digital Transformation on Business

Digital Technology has Enabled business to innovate their approach to interacting with society. People from all generations are more comfortable with digital technology and are using smart devices to their advantage Throughout their busy days.

Many companies now provide some or all of their services on-line. From the comfort of your home, car,gym, or office, you can shop for groceries on-line, order restaurant meals to be delivered to your door, book travel on-line, …

2.1.1.2.1. Sensors are everywhere

Smart homes can be equiped with motion sensors, water sensors, light sensors, doorbell sensors, temperature sensors, …
There can be sensors in traffic lights, transport trucks, parking garages, security cameras, trains and planes.
All of the sensors and measuring devices collect and transmit their data.
The data can be stored and analyzed at a later date or it can be analyzed immediately to be used to modify computers, mobile devices or precesses of any sort.

2..1.1.2.2. How is the stored and analyzed data used ?

- Businesses : determine buying patterns, forecast new trends, and streamline production
- Governements : monitor the environment, forecast population trends, predict crime rates, and plan for social services
- Cities : control traffic, monitor parking, provide police or fire support quicker, and control waste management

2.1.1.3. Can Smart Think ?

All digital devices work based on computer programs and supplied data. Artificial intelligence implies that these devices are able to think on their own. If programmed appropriately, smart devices are able to evaluate data that is provided to them and modify processes or settings « on the fly ». If they are provided with sufficient data, they can « learn » and modify their own code based on the new parameters.

Imagine a refrigerated transport truck, carrying frozen goods, that is equipped with a global positioning sensor. As the truck drivers into a majo city, the sensor determines that there is an accident ahead that is causing major traffic congestion. The sensor sends the data to the computer system that collects the data and make decisions. The system then alerts the driver to the new conditions so that the accident can be bypassed.

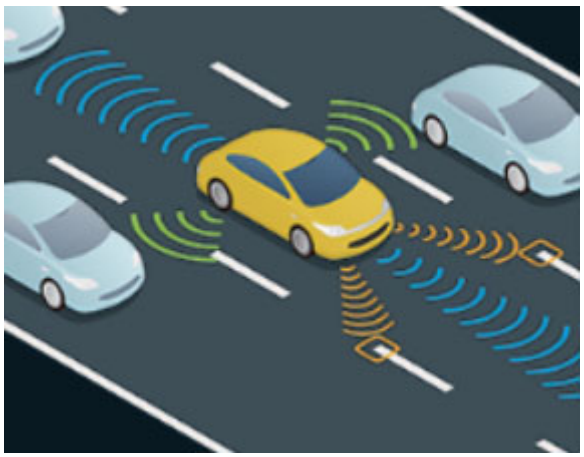
This automatic interaction has saved the driver time and will get the transported product to market faster with a product that is still frozen.

Corporate offices can be occupied by thousands of employees, keeping the environment, such as lighting, heat, humidity, in the building within acceptable parameters helps to keep employees happy and therefore more productive

Ideal building : https://cisco-netacad.wistia.com/medias/k7s8f8c9cj

Smart Cities, such as Barcelona, Spain, use sensors to control many of their infrastructure systems such as traffic flow, parking, water utilization and hydro

Example: Weight sensors in parking spaces allow drivers to quickly know where there is an available parking spot. This reduces driving and idling time for the driver and lowers carbon emissions for the environment



Self-driving cars are revolutionizing transportation. The cars are equipped with many ultrasound sensors, cameras, precision GPSs, and computers. The combination of the on-board equipment allows the computers to identify other cars, lanes, pedestrians, and obstructions.
This information allows the car to stay n its lane, stop when required, and weave around obstructions.

The road to complete autonomy using this technology is complicated. There have been many high-profile crashes and some serios accidents involving self-driving cars. Some states within the USA have already approved limited use of self-driving cars but researchers believe it will be a few years before he technology becomes mainstream.

Who is the next??? Airplanes? Trucks?

2.1.2. Globally connectaed through networks

2.1.2.1. Networking is the Foundation

Thirty billion things provide trillions of gigabytes of data. How can they work together to enhance our decision-making and 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 the digitized world.
The methods that we use to communicate continue to evolve. Whereas we were once limited by cables and plugs, breakthroughs in wireless and digital technology have significantly extended the reach of our communications.

Networks form the foundation of the digitized world. Networks come in all sizes. They can range from simple networks consisting of two computers to networks connecting millions of devices.
Simple networks in homes enable connectivity to the Internet. They also enable the sharing of resources, such as printers, documents, pictures, and music, between a few local computers.

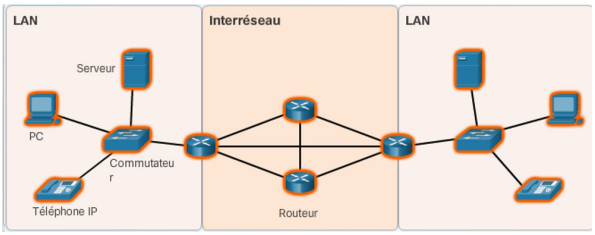
In businesses and large organizations, networks can provide products and services to customers through their connection to the Internet. Networks can also be used on an even broader scale to provide consolidation, storage, and access to information on network servers. Networks allow for email, instant messaging, and collaboration among employees. In addition, the network enables connectivity to new places, giving machines more value in industrial environments.

The Internet is the largest network in existence and effectively provides the “electronic skin” that surrounds the planet. 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 home networks connect to the Internet.

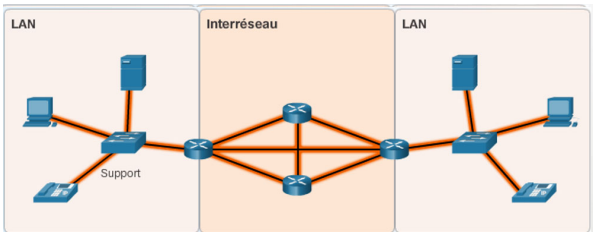
Components of a network

The path that a message takes from source to destination can be as simple as a single cable connecting one computer to another, or as complex as a network that literally spans the globe. This network infrastructure is the platform that supports the network. It provides the stable and reliable channel over which our communications can occur.

- 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.



Devices



Media

- 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. Processes are less obvious to us but are critical to the operation of networks.

End Devices

The network devices that people are most familiar with are called end devices. All computers connected to a network that participate directly in network communication are classified as hosts. 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 (smarthphones, 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 IoE

End devices are either the source or destination of data transmitted over the network. In order to distinguish one end device from another, each end device on a network is identified by an address. When an end device initiates communication, it uses the address of the destination end device to specify where the message should be sent.

A server is an end device that has software installed that enables it to provide information, like email or web pages, to other end devices on the network. For example, a server requires web server software to provide web services to the network.

A client is an end device that has software installed to enable it to request and display the information obtained from a server. An example of client software is a web browser, like Internet Explorer

Intermediate network devices

Intermediate devices interconnect end devices. These devices provide connectivity and work behind the scenes to ensure that data flows across the network. Intermediate devices connect the individual hosts to the network and can connect multiple individual networks to form an internetwork.

Examples of intermediate network devices and their roles are:

- Switches and wireless access points (Network Access)
- Routers (Internetworking)
- Firewalls (Security)

The management of data as it flows through the network is also a role of the intermediate device. These devices use the destination host address, in conjunction with information about the network interconnections, to determine the path that messages should take through the network.

Processes running on the intermediate network devices perform these functions:

- Regenerate and retransmit data signals
- Maintain information about what pathways exist through the network and internetwork
- Notify other devices of errors and communication failures
- Direct data along alternate pathways when there is a link failure
- Classify and direct messages according to Quality of Service (QoS) priorities
- Permit or deny the flow of data, based on security settings

Network Media

Communication across a network is carried over a medium, such as through a cable or through the air. The medium facilitates communication from source to destination.
Modern networks primarily use three types of media to interconnect devices and to provide the pathway over which data can be transmitted.

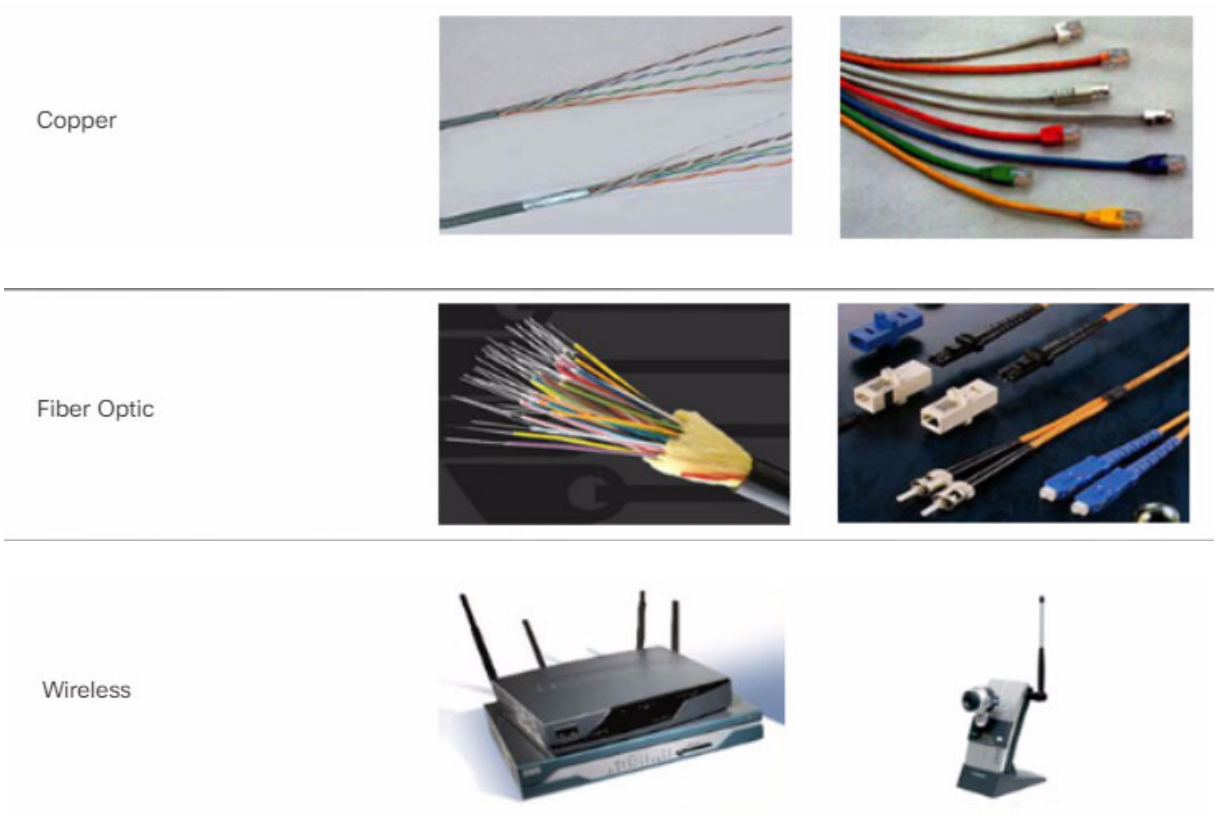
As shown in the figure, these media are:

- Metallic wires within cables
- Glass or plastic fibers (fiber optic cable)
- Wireless transmission

The signal encoding that must occur for the message to be transmitted is different for each media type. On metallic wires, the data is encoded into electrical impulses that match specific patterns. Fiber optic transmissions rely on pulses of light, within either infrared or visible light ranges. In wireless transmission, patterns of electromagnetic waves depict the various bit values.
Different types of network media have different features and benefits. Not all network media have the same characteristics, nor are they appropriate for the same purposes.

The criteria for choosing network media are:

- The distance the media can successfully carry a signal
- The environment in which the media is to be installed
- The amount of data and the speed at which it must be transmitted
- The cost of the media and installation



Classify the Network components

Device Type Representation	End Device	Intermediate Device
 Wireless Access Point		
 Laptop		
 Switch		
 Server		
 Smartphone		
 Router		
 Printer		
 Firewall		

Networking types

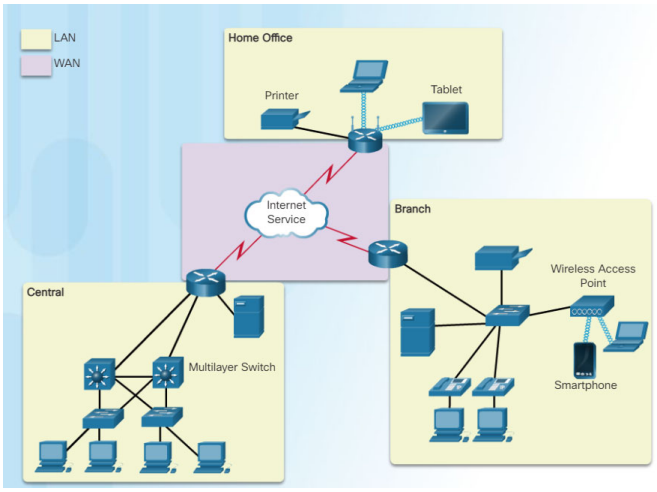
Modern networks can be a bit confusing. There are many types that are characterized by their geographic size, by the number of devices or networks that they connect, and by whether they support mobile devices or not. Networks can also be characterized by their function and purpose.

- **Personal Area Network (PAN)**

Personal area networks are small networks where connected wireless devices are within personal reach (Figure 1). Connecting your smartphone to your car using Bluetooth is an example of a PAN.

- **Local Area Network (LAN)**

LANs are typically networks in a small or local geographic area, such as a home, small business or department within a large corporation (Figure 2). LANs can connect two or more devices, including computers, printers, and wireless devices. LANs provide access to larger wide area networks (WANs) and the Internet.



- **Wide Area Networks (WANs)**

The term WAN typically refers to a collection of LANs that provides inter-LAN and Internet connectivity for businesses and governments.

- **Internet**

The Internet is a multi-layer global network system that connects hundreds of millions of computers (Figure 3). The Internet is not owned by any one person or organization. This large system is comprised of multiple local and global networks serving private, public, business, academic, and government purposes. It allows for the exchange of data between more than a hundred Internet-linked countries worldwide. This makes the Internet an enormous carrier of various information resources and services. Some of these include text and multi-media data, email, online chat, VoIP, file transfer and file sharing, ecommerce, and online gaming.

- **Wireless Networks**

Wireless networks are those computer networks that use electromagnetic waves instead of wires in order to carry signals over the various parts of the network. Wireless networks can be described as PANs, LANs or WANs, depending on their scope.

Because browsing the Internet is considered a normal daily activity, wireless access points have become common place in the communication infrastructure today. Public Internet-connected places include libraries, airports, coffee shops, hotels, and specialized Internet cafes. Thanks to Wi-Fi technology, the Internet can now be accessed by every person with a laptop, tablet, or smartphone. Figure 4 shows the different categories of wireless networks that are available.

Wireless Networks

Type	Range	Standards
Personal area network (PAN)	Within reach of a person	Bluetooth, ZigBee, NFC
Local area network (LAN)	Within a building or campus	IEEE 802.11 (WiFi)
Metropolitan area network (MAN)	Within a city	IEEE 802.15 (WiMAX)
Wide area network (WAN)	Worldwide	Cellular (UMTS, LTE, etc.)

- **The Cloud**

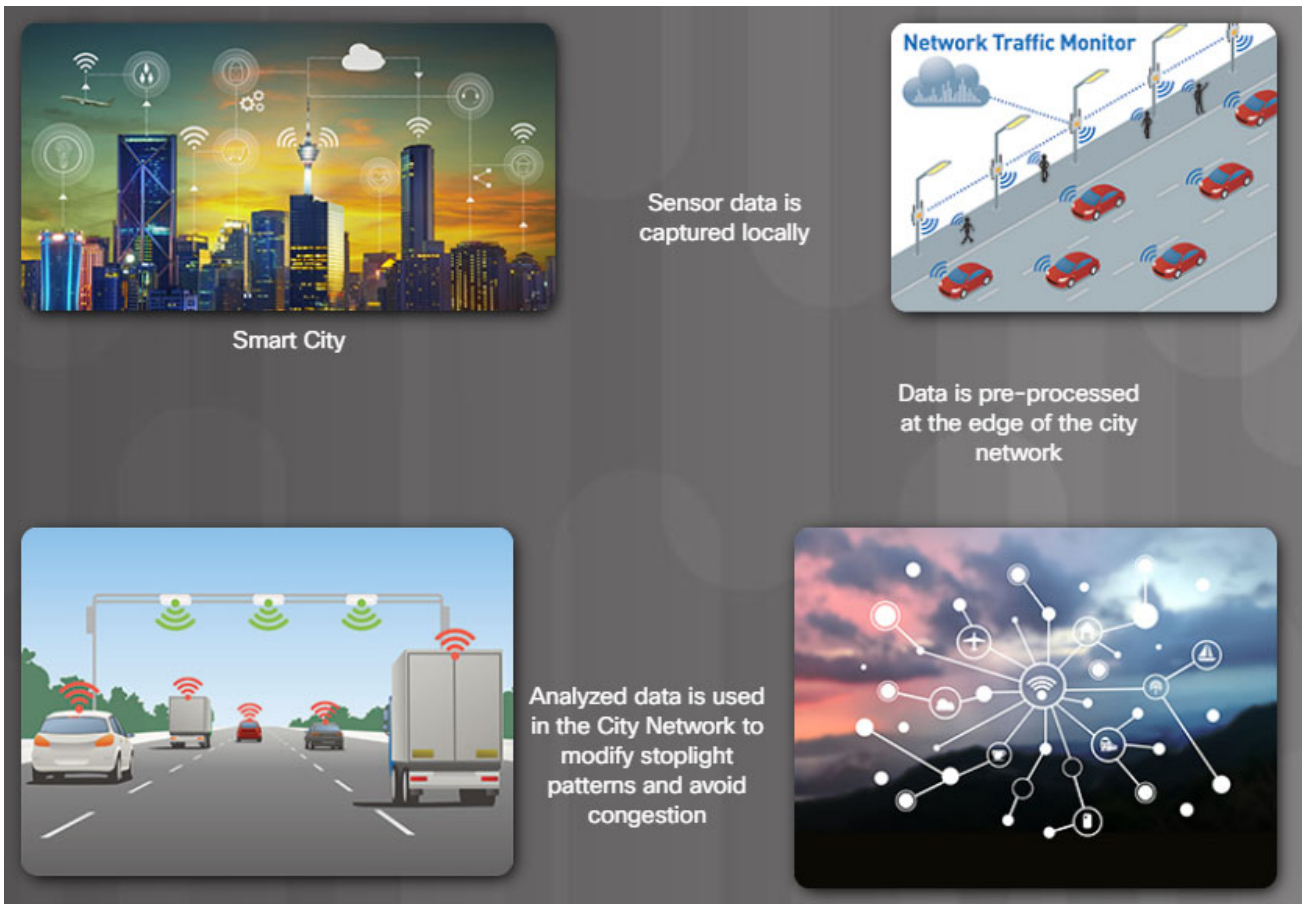
The term “cloud” is used in many different ways. The cloud is not as much a type of network as it is a collection of data centers or groups of connected servers that are used to store and analyze data, provide access to on-line applications, and provide backup services for personal and corporate use (Figure 5). Cloud services are provided by different organizations.

- **The Edge**

The edge refers to the physical “edge” of a corporate network.

- **Fog Computing**

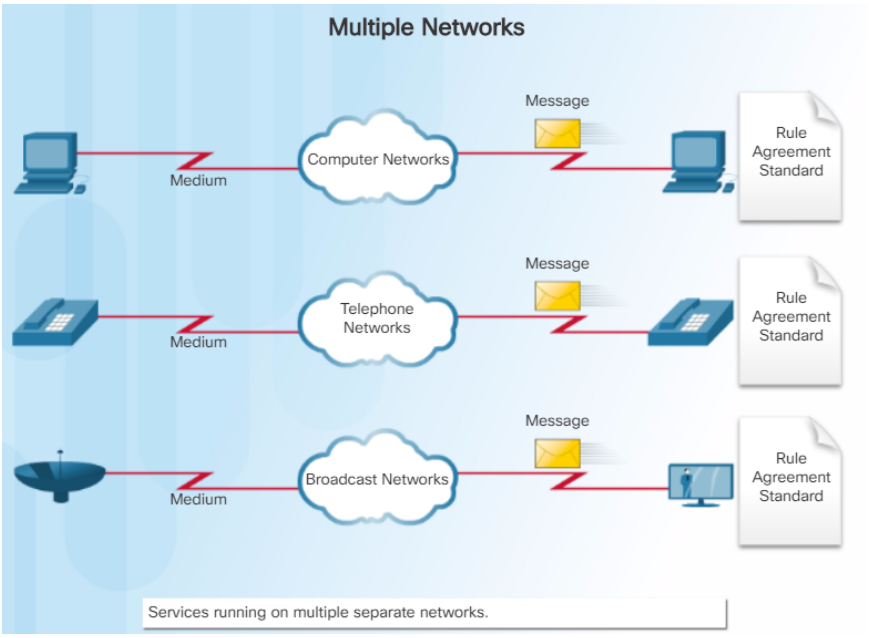
With the rising number of sensors used by the Internet of Things, there is often a need to store the sensor data securely and closer to where the data can be analyzed. This analyzed data can then be used quickly and effectively to update or modify processes within the organization. Figure 6 shows an example of a smart city and how sensor data is processed. The fog is located at the edge of a business or corporate network. Servers and computer programs allow the data to be pre-processed for immediate use. Then the pre-processed data can be sent to the cloud for more in-depth computing if required.



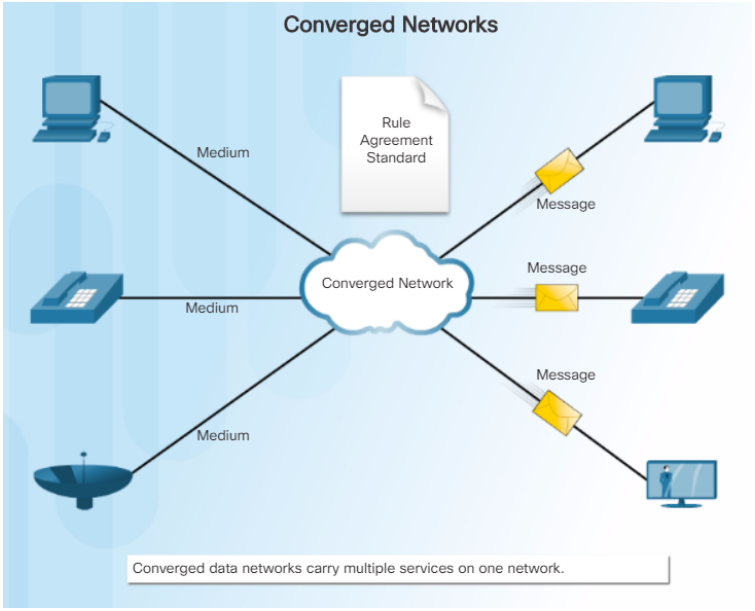
The converged Network

Modern networks are constantly evolving to meet user demands. Early data networks were limited to exchanging character-based information between connected computer systems. Traditional telephone, radio, and television networks were maintained separately from data networks. In the past, every one of these services required a dedicated network, with different communication channels and different technologies to carry a particular communication signal. Each service had its own set of rules and standards to ensure successful communication.

Consider some schools that were cabled for a computer network thirty years ago. Classrooms were cabled for the computer network. They were also cabled for a telephone network. And, they were cabled for a video network. These networks were disparate; meaning that they could not communicate with each other, as shown in Figure.



Advances in technology are enabling us to consolidate these different kinds of networks onto one platform referred to as the "converged network." Unlike dedicated networks, converged networks are capable of delivering voice, video, text, and graphics between many different types of devices over the same network, as shown in Figure. Previously separate and distinct communication forms have converged onto a common platform. This platform provides access to a wide range of alternative and new communication methods that enable people to interact directly with each other almost instantaneously.



On a converged network there are still many points of contact and many specialized devices, such as personal computers, phones, TVs, and tablet computers, but there is one common network infrastructure. This network infrastructure uses a common set of rules, agreements, and implementation standards.

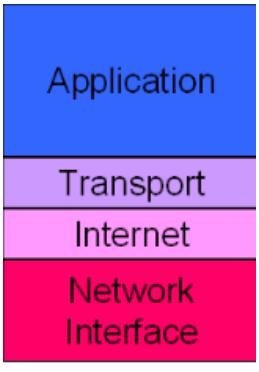
Protocol suite

Networking protocol suites describe processes, such as:

- The format or structure of the message
- The method by which networking devices share information about pathways with other networks
- How and when error and system messages are passed between devices
- The setup and termination of data transfer sessions

Protocol suites can be implemented in hardware or software, or a combination of both. Each layer is responsible for part of the processing to prepare data for transmission across the network.

One of the most common networking protocol suites is known as Transmission Control Protocol/Internet Protocol (TCP/IP). All devices that communicate across the Internet must use the TCP/IP protocol suite. Specifically, they must all use the IP protocol from the Internet layer of the stack, as this allows them to send and receive data over the Internet.



TCP/IP

The TCP/IP model describes the rules that the TCP/IP protocol suite encompasses. The Internet Engineering Task Force (IETF) defines the TCP/IP model. To learn more about the layers of the TCP/IP model, click each layer in Figure 1.

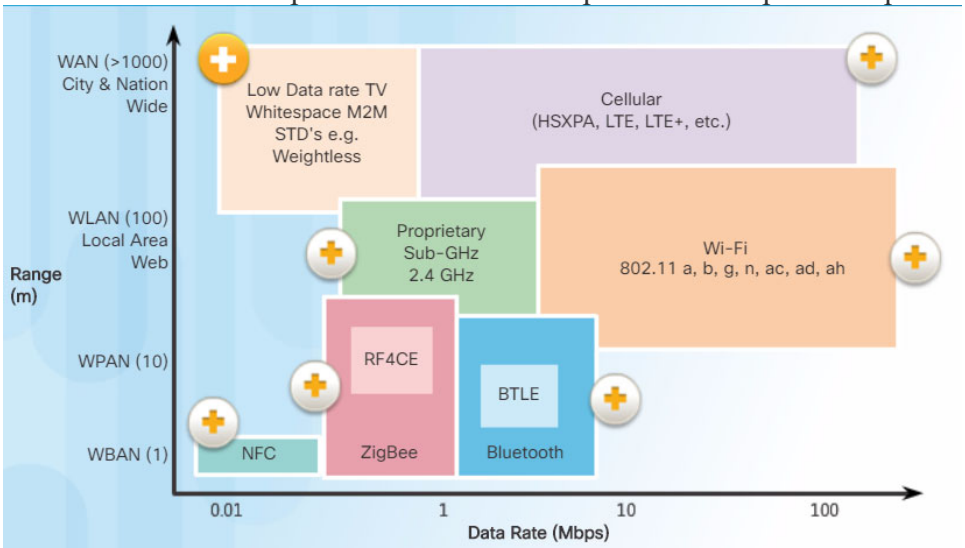
Objects that are IP-enabled, meaning that necessary TCP/IP software is installed, will have the ability to forward data across the Internet directly. Examples of these devices are shown in Figure 2.

Network connectivity

The bottom layer of the TCP/IP model is network access. Network access covers the protocols that devices must use when transferring data across the network. At the network access layer, devices can be connected to the network in one of two ways: wired and wireless.

The most commonly implemented wired protocol is the Ethernet protocol. Ethernet uses a suite of protocols that allow network devices to communicate over a wired LAN connection. An Ethernet LAN can connect devices using many different types of wiring media.

There are a number of wireless network protocols available today. The characteristics of these protocols vary greatly. Figure 2 provides a few common wireless protocols and shows a visual representation of where these protocols fit in the classification spectrum. Notice that a protocol can span multiple classifications.



In addition to these protocols, there are other network access layer protocols that are available in both wired and wireless form.

- **Weightless :** Use the unused portions of the spectrum band in and around TV transmissions. It is a low frequency band which enables excellent propagation without needing antennas in devices. It has relatively low output power.
-
- **Cellular :** The technology behind cell phones is widespread and readily available. Cellular networks are proven, reliable, and provide coverage over vast areas. Some IoT designs are already using consumer cell phones for their connectivity.
-
- **Proprietary :** This is a communications protocol owned by a single organization or individual
- **Wi-Fi :** This is the name of a popular wireless networking technology that uses radio waves to provide wireless high-speed Internet and network connections.
-
- **NFC :** Near Field Communications is a set of standards for establishing radio communications between devices by touching them together or bringing them into proximity, usually no more than a few inches.
-
- **ZigBee :** This is a specification for a suite of high-level communication protocols used to create personal area networks built from small, low-power digital radios.
-
- **Bluetooth :** Bluetooth Low Energy (BTLE) is being adopted by the health care industry for portable medical and lifestyle devices.

Network access for currently unconnected things

For objects with extremely low power requirements to send information across the network, several short-range wireless communication protocols exist. In some cases, these protocols are not IP-enabled and must forward information to a connected IP-enabled device, such as a controller or gateway.

- **Lowpan :** 6LoWPAN arose from the need to include extremely low-powered devices with limited processing capabilités as part of IoT, for example, smart meters in a small networks.

- **Bluetooth :** This protocol is typically used between devices that are in close range, such as a smartphone connecting to a Bluettoth-enabled headset, or a Bluetooth-enabled wireless keyboard connected to a computing device.

- **ZigBee :** is a another example of an 802.15 protocol suite that uses pairing between a specified source and destination. An example is between a door sensor and a security system that sends an alert when the door is opened.

- **NFC :** Near Field Communication is a standard for communicating between things in very close proximity, usually within a few inches. For example, NFC works at point of sale between an RFID tag and the reader.

2.2. Devices that connect to the IoT

2.2.1. The growth of IoT Devices

2.2.1.1. What is the Iot ?

he Internet of Things (IoT) is the connection of millions of smart devices and sensors connected to the Internet. These connected devices and sensors collect and share data for use and evaluation by many organizations. These organizations include businesses, cities, governments, hospitals and individuals. The IoT has been possible, in part, due to the advent of cheap processors and wireless networks. Previously inanimate objects such as doorknobs or light bulbs can now be equipped with an intelligent sensor that can collect and transfer data to a network.

Researchers estimate that over 3 million new devices are connected to the Internet each month. Researchers also estimate that in the next four years, there are going to be over 30 billion connected devices worldwide. Perhaps a third of connected devices will be computers, smartphones, tablets, and smart TVs. The remaining two-thirds will be other kinds of “things”: sensors, actuators, and newly invented intelligent devices that monitor, control, analyze, and optimize our world.

Some examples of intelligent connected sensors are: smart doorbells, garage doors, thermostats, sports wearables, pacemakers, traffic lights, parking spots, and many others. The limit of different objects that could become intelligent sensors is limited only by our imagination.

2.2.1.2. Many different organizations are benefitting from the data collected, saved, and analyzed from sensors

- Businesses have more information about products that they sell and who is purchasing them. Armed with this type of data, they can streamline production and target their marketing and advertising to specific areas or audiences, promotes creation of new business opportunities and marketing ideas.
- Retailers are able to do more target marketing reduce losses based on unsold products, and can provide loyalty bonuses for preferred or frequent customers, as well as manage types of in-store products
- Manufacturing saves money, improves efficiency, and improves productivity of manufacturing processes and operations. Manufacturers reduce downtime by predicting maintenance requirements and improving scheduling of field services employees.
- Governments monitor environmental issues, target funding for social issues, and have informed control of power output

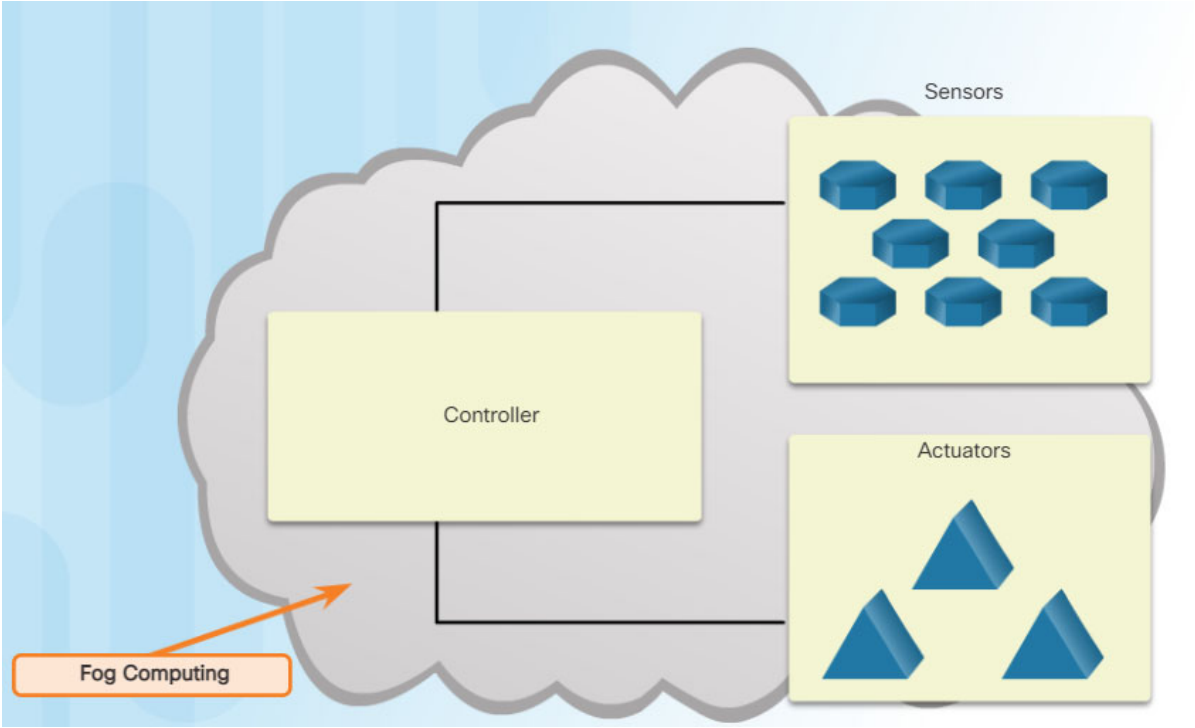
- Cities have the ability to control traffic patterns based on time of day or major events, monitor and control garbage and recycling, monitor health and housing needs, and evaluate future transportation requirements.
- Individuals can reap improved fitness and health benefits, better home and family security and reduced costs for energy and heating systems. They can enjoy more varied entertainment, limit the speed a teenage driver can reach or even monitor the health of and older family member at the wheel of their car.

2.2.1.3. How are Iot devices connected to the network?

A sensor needs to be connected to a network so that the gathered data can be stored and shared. This requires either a wired Ethernet connection or a wireless connection to a controller. Controllers are responsible for collecting data from sensors and providing network or Internet connectivity. Controllers may have the ability to make immediate decisions, or they may send data to a 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.

Sensors often work together with a device called an actuator. Actuators take electrical input and transform the input into physical action. As an example, if a sensor detects excess heat in a room, the sensor sends the temperature reading to the microcontroller. The microcontroller can send the data to an actuator which would then turn on the air conditioner.

The majority of new devices such as fitness wearables, implanted pacemakers, air meters in a mine shaft, and water meters in a farm field all require wireless connectivity. Because many sensors are “out in the field” and are powered by batteries or solar panels, consideration must be given to power consumption. Low-powered connection options must be used to optimize and extend the availability of the sensor.



2.2.1.4. The future of networks

Networks are now connecting billions of sensors. Through software, the data from these sensors can cause changes to physical environments without human intervention.

As was mentioned previously, all digital devices work based on computer programs and supplied data. Artificial Intelligence implies that these devices are able to think on their own. If programmed appropriately, smart devices are able to evaluate data that is provided to them and modify processes or settings immediately. If they are provided with sufficient data, they can "learn" and modify their own code based on the new parameters.

So what comes next?
We know that software can be written to let data modify parameters within code for changing the temperature setting in your home or the speed with which your teenager can drive the family car. Why could we not provide software with rules, guidelines, or intent so that data could modify the network, infrastructure features, or security features within a network? This is actually already possible. It is called Intent-Based Networking (IBN).

Here is a simple example to better understand the concept of IBN: The business may define that a contract employee is given access to only a specific set of data and applications. This is the **intent**. In an intent-based networking system (IBN), all the network devices will be automatically configured to fulfil this requirement across the network, no matter where the employee is connected. VLAN, subnet, ACL and all other details will be automatically defined and configured following best practices. The intent has to be defined once in a central management console, and then, the network will continuously assure it, even if there are changes in the network.

2.3. Summary

The world is quickly being covered with networks which allow digital devices to interconnect and transmit. As digital networks continue to grow around the world, and as the economic benefits of digitization continue to grow, we are seeing a digital transformation. Digital transformation is the application of digital technology to provide the stage for business and industry to innovate.

Sensors are now everywhere, collecting and transmitting massive amounts of data. The generated data can be stored and analyzed at a later date, or it can be analyzed and used immediately. Sensors can be in the home, on traffic lights, in farm fields, and on our bodies. The analyzed data is used by governments, cities, businesses, and individuals to effect changes such as monitoring the environment, forecasting population growth, controlling waste management, or securing a home.

Networks form the foundation of the digitized world. There are many types of networks that are characterized by their geographic size, by the number of devices or networks that they connect, and by whether they support mobile devices or not. Networks can also be characterized by their function and purpose.

- PAN: Bluetooth
- LAN
- WAN: Internet, the cloud, fog computing
- Wireless: Wi-Fi, Cellular

A sensor typically connects to a controller using a wireless connection. Controllers collect data from sensors and send the data for storage or analysis. Controllers may have the ability to make immediate decisions, or they may work together with a device called an actuator. Actuators take electrical input and transform the input into physical action.

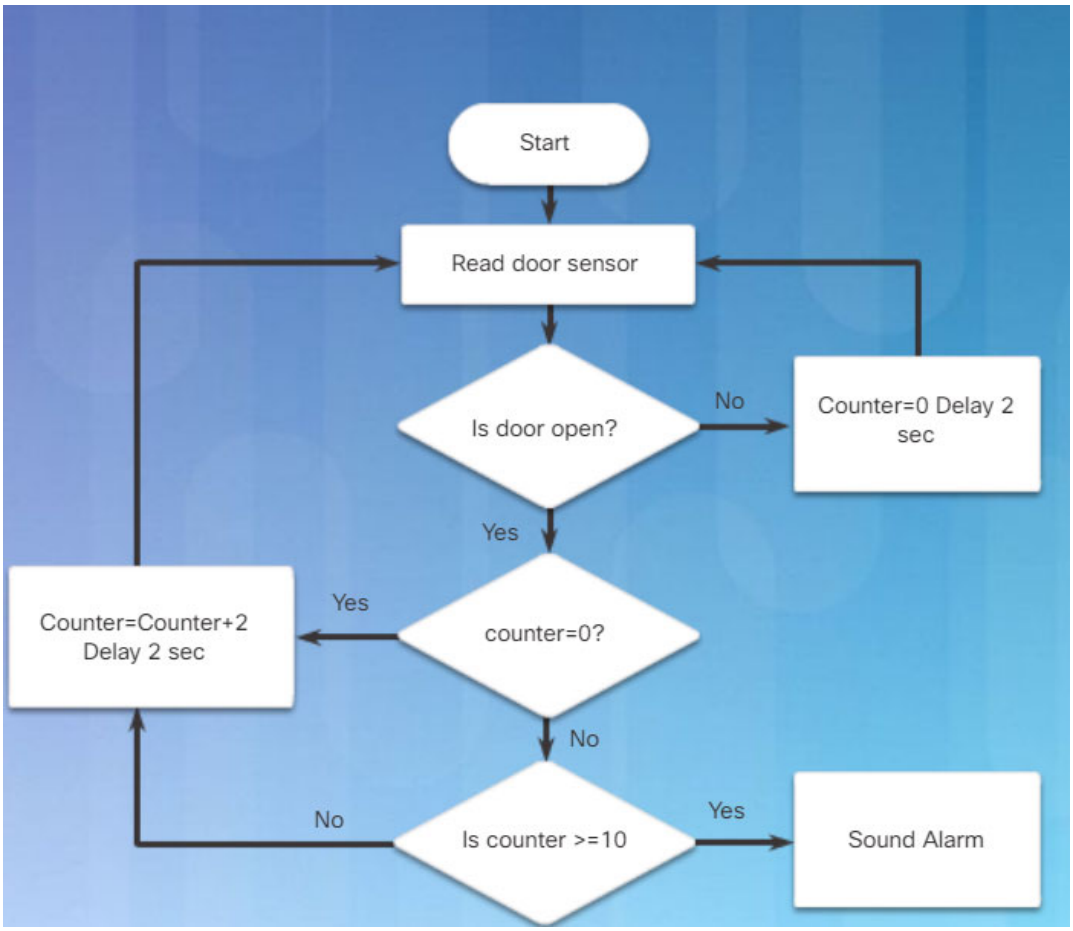
Networks are now connecting billions of sensors and have the ability to make changes to physical environments without human intervention. The future of networking will revolve around artificial intelligence (AI) and intent-based networking (IBN). If programmed appropriately, smart devices are able to evaluate data that is provided to them and modify processes or settings. If they are provided with sufficient data, they can “learn” and modify their own code based on the new parameters.

3. Everything becomes programmable

3.1. Apply Basic programing to support IoT devices

3.1.1. Basic programming concepts

3.1.1.1. Follow the Flowcharts



Answer the following questions based on the supplied flowchart?

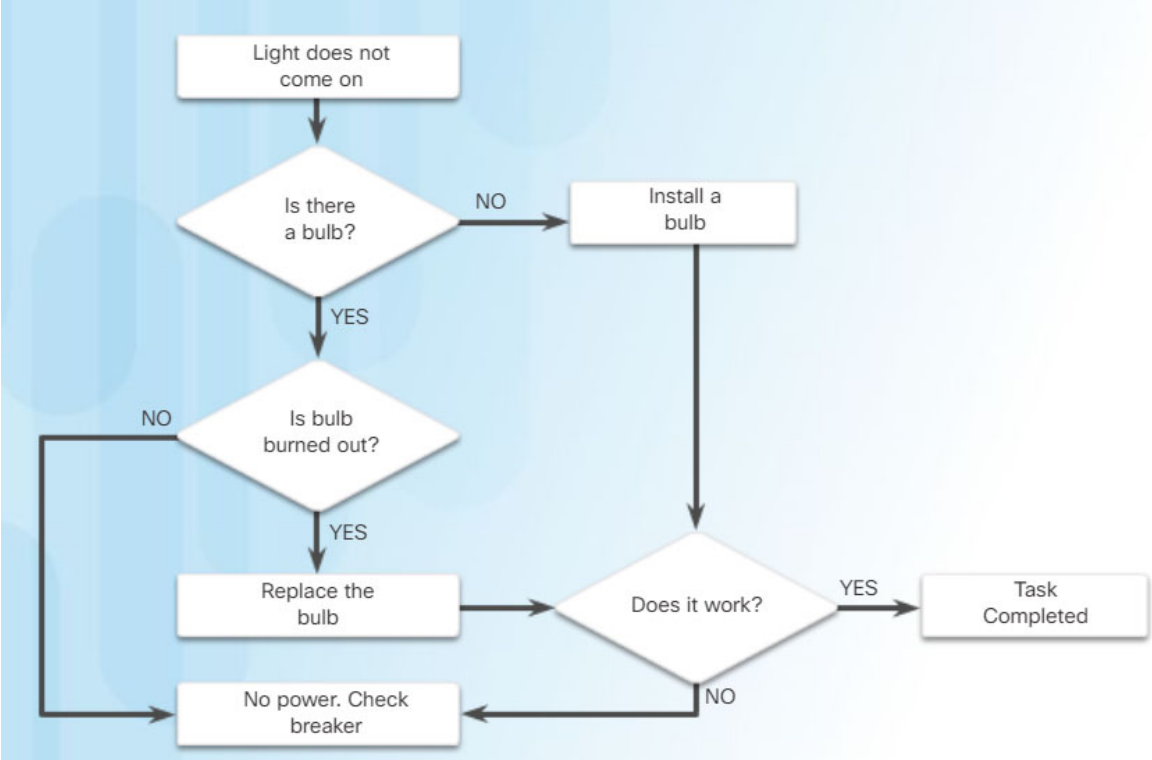
- Is the sensor checking for an open or a closed door?
- How frequently is the sensor checked?
- Will the alarm sound if the door is open for 5 seconds?
- Will the alarm sound if the door is open for 10seconds?
- Will the alarm sound if the door is open for 5 seconds, shut for 5 secondes, then reopened for 5 seconds?

3.1.1.2. Flowcharts

Flowcharts are used in many industries including engineering, physical sciences, and computer programming where a complete understanding of processes or workflows is required. Flowcharts are diagrams that are used to represent these processes or workflows.
Flowcharts illustrate how a process should work. Flowcharts should not require complex, industry-specific terminology or symbols. A flowchart should be easy to understand without having to be an expert in the chosen field.

Flowcharts should show input states, any decisions made, and the results of those decisions. It is important to show the steps that should be taken when the result of a decision is either yes or no.

It is common for programmers to create a first draft of a program in no specific programming language. These language-independent programs are focused on the logic rather than in the syntax and are often called algorithms. A flowchart is a common way to represent an algorithm. An example of a flowchart is shown in the figure.



Example of a flowchart. Rectangles represent actions. Diamonds represent decisions

3.1.1.3. System software, application software, and computer languages

There are two common types of computer software: system software and application software. Application software programs are created to accomplish a certain task or collection of tasks. For example, Cisco Packet Tracer is a network simulation program that allows users to model complex networks and ask "what if" questions about network behavior.

System software works between the computer hardware and the application program. It is the system software that controls the computer hardware and allows the application programs to function. Common examples of system software include Linux, Apple OSX, and Microsoft Windows.
Both system software and application software are created using a programming language. A programming language is a formal language designed to create programs that communicate instructions to computer hardware. These programs implement algorithms which are self-contained, step-by-step sets of operations to be performed.

Some computer languages compile their programs into a set of machine-language instructions. C++ is an example of a compiled computer language. Others interpret these instructions directly without first compiling them into machine language. Python is an example of an interpreted programming language. An example of Python code is shown in the figure.

When the programming language is determined and the process is diagrammed in a flowchart, program creation can begin. Most computer languages use similar program structures.

```
year = int(input("Enter a year to check if it is a leap year\n"))
if (year % 4) == 0:
   if (year % 100) == 0:
       if (year % 400) == 0:
           print("{0} is a leap year".format(year))
       else:
           print("{0} is not a leap year".format(year))
   else:
       print("{0} is a leap year".format(year))
else:
   print("{0} is not a leap year".format(year))
```

Program to verify leap years in Python

3.1.1.4 Programming Variables

Programming languages utilize variables as dynamic buckets to hold phrases, numbers, or other important information that can be used in coding. Instead of repeating specific values in numerous places throughout the code, a variable can be used. Variables can hold the result of a calculation, the result of a database query, or some other value. This means that the same code will function using different pieces of data without having to be rewritten.

For instance "x + y = z" is an example of a programming expression. In this expression, x, y and z are variables which can represent characters, character strings, numeric values or memory addresses.
A variable can refer to a value. For instance the expression "a = 10" associates the value 10 to variable a.
A variable can also represent a memory location. The expression "a = 10" represents that the value 10 is stored in some location of the computer memory, which is referred to as 'a'.
Variables can be classified into two categories:

- **Local Variables** - These are variables that are within the scope of a program / function / procedure.
- **Global Variables** - These are variables that are in the scope for the time of the program's execution. They can be retrieved by any part of the program.

Variables allow programmers to quickly create a wide range of simple or complex programs which tell the computer to behave in a pre-defined fashion.

3.1.1.5. Basic program structures

People impart logic to computers through programs. Using specific logic structures, a programmer can prepare a computer to make decisions. The most common logic structures are:

- **IF – THEN** - This logic structure allows the computer to make a decision based on the result of an expression. An example of an expression is myVar > 0. This expression is true if the value stored in the myVar variable is greater than zero. When an IF-THEN structure is encountered, it evaluates the provided expression. If the expression is false, the computer moves on to the next structure, ignoring the contents of the IF-THEN block. If the expression is true, the computer executes the associated action before moving on to the next instruction in the program.

```
IF (value1 > value2) THEN print_on_the_screen "Value1 is greater than Value2"
```

- **FOR Loops** – These are used to execute a specific set of instructions a specific number of times, based on an expression. The term loop comes from the fact that the set of instructions is executed repeatedly. While the syntax of FOR loops varies from language to language, the concept remains the same. A variable acts as a counter inside a range of values identified by a minimum and a maximum. Every time the loop is executed, the counter variable is incremented. When the counter is equal to the defined maximum value, the loop is abandoned and the execution moves on to the next instruction.

```
FOR (i=0; i < 100; i++) {
   print_on_the_screen "counter =" + i
}
```

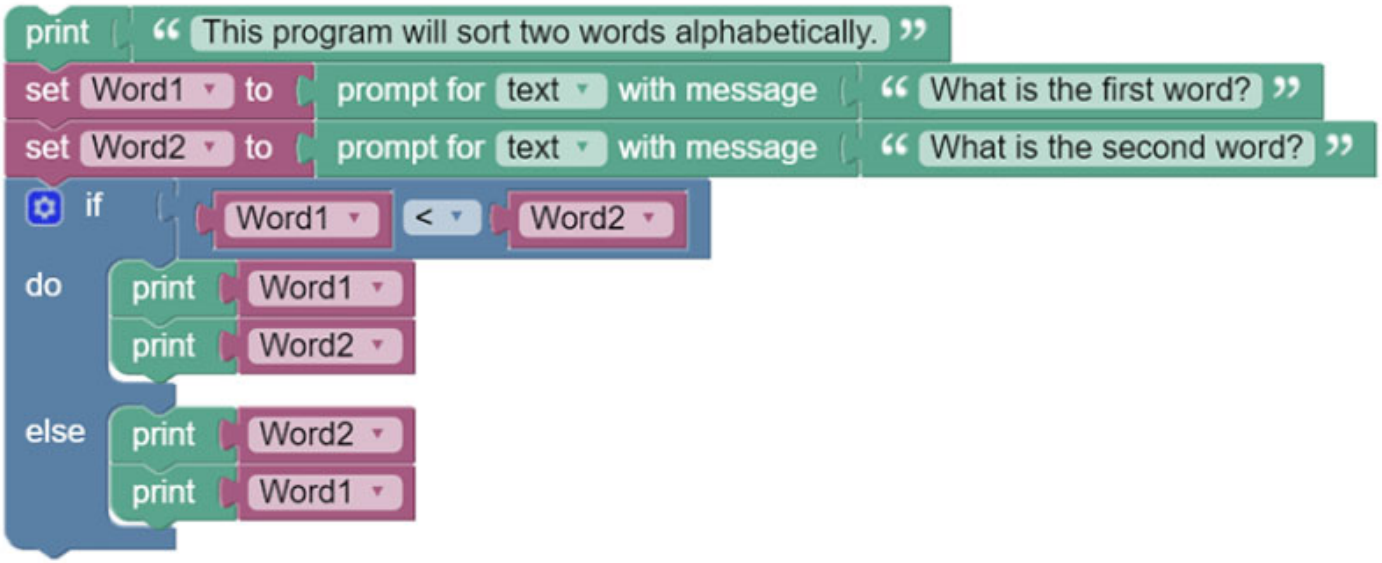
- **WHILE Loops** – These are used to execute a specific set of instructions while an expression is true. Notice that often the instructions inside the loop will eventually make the expression evaluate as false.

```
WHILE (value < 10) {
   print_on_the_screen "Value is still less than 10"
   value = value + 1
}
```

3.1.2. Basic programing using Blockly

3.1.2.1. What is Blockly ?

Blockly is a visual programming tool created to help beginners understand the concepts of programming. By using a number of block types, Blockly allows a user to create a program without entering any lines of code.



Blockly implements visual programming by assigning different programming structures to colored blocks. The blocks also contain slots and spaces to allow programmers to enter values required by the structure.

Programmers can connect programming structures together by dragging and attaching the appropriate blocks. Programming structures such as conditionals, loops, and variables are all available for use.

Creating a new variable in Blockly is a simple matter of dragging the variable block onto the work space and filling in the value slot. It is also possible to change the contents of a variable as the program is being executed.

Blockly also supports functions. Similar to the variables, Blockly has specific blocks to represent functions. Also similar to variables, programmers simply select and drag function blocks to the work space and fill in the required slots.

Notice in Figures that the variable block and the print on screen block both have a bevel tab on the bottom and a slot on the top. This means that the two blocks can be snapped together to create a program sequence. Blockly will execute the block on the top first, then move on to the block below it.
Other blocks are available such as an IF THEN block, a WHILE block and a FOR block. There are also blocks specifically for sensors and actuators.

Blockly can be used to translate the block-based code into Python or JavaScript. This is very useful to beginner programmers.

3.1.2.2. Blockly Games

Google provides a series of free and open source educational games that can help you learn programming. The series is called Blockly Games.

There are a number of levels to complete to help you get started. Blockly may look like a toy, but it is a great tool to improve your logical thinking skills, which is one of the building blocks of computer programming.

https://blockly.games/

3.1.3. Programing with Python

3.1.3.1. What is python?

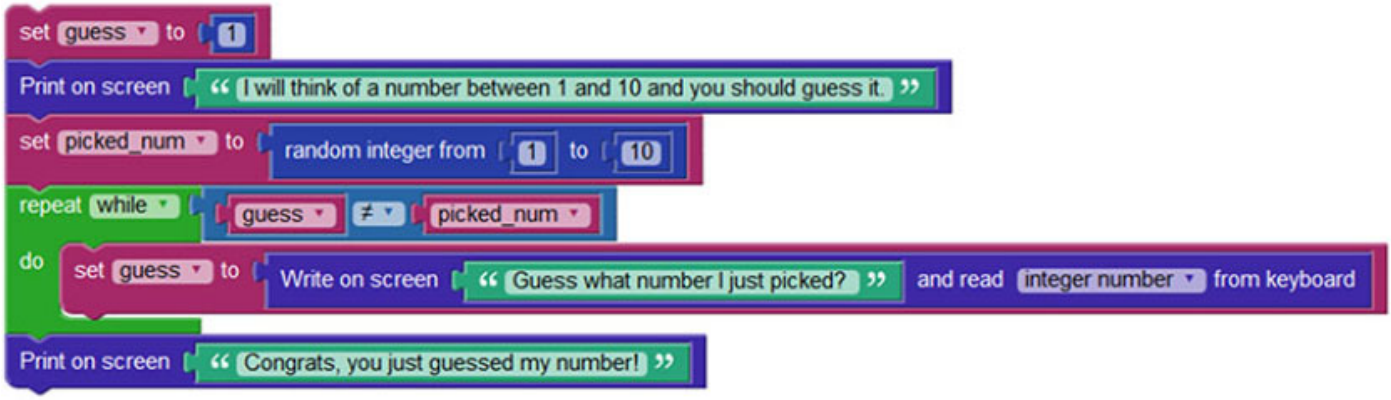
Python is a very popular language that is designed to be easy to read and write. Python's developer community adds value to the language by creating all types of modules and making them available to other programmers.

The core philosophy of the language is summarized by the document https://www.python.org/dev/peps/pep-0020/ :

- Beautiful is better than ugly
- Explicit is better than implicit
- Simple is better than complex
- Complex is better than complicated
- Readability counts

Despite the fact Python is designed to be easy, there is still a learning curve. To make it easier to learn Python, a beginner can use Blockly to enhance his or her Python understanding.
While different programming languages have different semantics and syntax, they all share the same programming logic. Beginners can use Blockly to easily create a language-independent program, export it as Python code and use this newly created code to learn about Python syntax, structure and semantics.

Blocky to python




```
import random

guess = None
picked_num = None


guess = 1
print('I will think of a number between 1 and 10 and you should guess it.')
picked_num = random.randint(1, 10)
while guess != picked_num:
  guess = int(input ('Guess what number I just picked? '))
print('Congrats, you just guessed my number!')
```

3.1.3.2. Variables and basic statements in Python

The interpreter receives and executes statements interactively.

The interpreter acts as a simple calculator. You can type an expression on it and it will write the value. Expression syntax is straightforward. The operators +, -, * and / work just as they do in most other languages (for example, Pascal or C). Parentheses (()) can be used for grouping.

Python's interactive mode implements the special variable "_" to hold the result of the last expression issued.

Variables are labeled memory areas that are used to store runtime program data. To assign values to variables in Python, use the equal to (=) sign. No result is displayed before the next interactive prompt.

Attempts to use a not defined variable (no assigned value), will result in an error.
Strings, defined as a sequence of characters, can also be handled by interactive mode. Use the backslash character (\) to escape characters. As an example, a string uses double quotes but also needs to use a double quote within the string. If the string is entered as follows: **"I really "need" this."**. Python will get confused and think that the first double quote within the string actually ends the string. If you place a backslash (\) before the double quotes inside the string as follows: **"I really \"need\" this"**, the backslash (\) causes Python to escape or ignore the character that follows.

Single quotes or double quotes can be used to wrap strings.

The print statement prints the result of the expression it was given. It differs from just writing the expression you want to write (as we did earlier in the calculator examples) in the way it handles multiple expressions and strings. Strings are printed without quotes, and a space is inserted between items, so you can format things nicely.

```
# Function to add two numbers:
def add_nums():
    a = 5
    b = 11
return a+b
>>> print (add_nums())
16
>>>
```

Functions are an important part of many programming languages. Functions allow for a block of code to be given a name and re-used as needed. Figure defines a function to add two numbers and print the result.

3.1.3.3. Useful functions and data types in python

Python supports many useful functions and datatypes. Some of the more important ones are as follows:

Range()
The range() function generates a list of numbers usually used to iterate with FOR loops.

- **range(stop)** - This is the number of integers (whole numbers) to generate, starting from zero.
- **range([start], stop, [step])** – This is the starting number of the sequence, the ending number in the sequence, and the difference between each number in the sequence.

Tuples
A tuple is a sequence of unchangeable Python objects. Tuples are sequences, separated by parentheses.

Lists
Lists are a sequence of changeable Python objects. Lists can be created by putting different comma-separated values between square brackets

Sets
Sets are unordered collections of unique elements. Common uses include membership testing, removing duplicates from a sequence, and computing standard math operations on sets such as intersection, union, difference, and symmetric difference.

Dictionary
A dictionary is a list of elements that are separated by commas. Each element is a combination of a value and a unique key. Each key is separated from its value by a colon. The entire dictionary is written within braces. Dictionary elements can be accessed, updated, and deleted. There are also many built-in dictionary functions such as a function that compares elements within different dictionaries and another that provides a count of the total number of elements within a dictionary.

3.1.3.4. Programing structure in Python

Similar to other languages, Python implements an IF-THEN structure. IF-THEN blocks can be used to allow the code to make decisions based upon the result of an expression.

The code performs a few tests and prints a message in accordance with the results of the test. Notice that Python also implements two sub-structures named ELSE and ELIF. ELSE allows the programmer to specify instructions to be executed if the expression is false. Short for ELSE IF, ELIF is used to perform a second test in case the first expression is false and another test is required. There can be zero or more ELIFs, and the ELSE part is optional.

```
>>> x = int(input("Please enter an integer: "))
Please enter an integer: 42
>>> if x < 0:
...     x = 0
...     print ('Negative changed to zero')
... elif x == 0:
...     print ('Zero')
... elif x == 1:
...     print ('Single')
... else:
...     print ('More')
...
More
```

The FOR loop in Python iterates the items of any sequence (a list or a string), in the order that they appear in the sequence.

```
>>> # Measure some strings:
... words = ['cat', 'window', 'defenestrate']
>>> for w in words:
...     print (w, len(w))
...
cat 3
window 6
defenestrate 12
```

The WHILE loop executes a block of code if the expression is true. The program shown in Figure uses a WHILE loop to calculate and print an initial sub-sequence of a Fibonacci series in which each number in the series is the sum of the previous two.
The third line contains a multiple assignment operator. The variables **a** and **b** get the new values of 0 and 1 in a single statement.

The WHILE loop calculates the next term in the Fibonacci series while the condition b < 10 is true. As in C, Python assumes any non-zero integer value as true and zero as false. The test used in the figure is a simple comparison.

```
>>> # Fibonacci series:
... # the sum of two elements defines the next
... a, b = 0, 1
>>> while b < 10:
...     print (b)
...     a, b = b, a+b
...
1
1
2
3
5
8
```

Notice that the body of the loop is indented. Indentation is Python's way of grouping statements. At the interactive prompt, you have to type a tab or space(s) for each indented line. More complicated input for Python should be done with a text editor. When a compound statement is entered interactively, it must be followed by a blank line to indicate completion (because the parser cannot guess which line will be the last line). Note that each line within a basic block must be indented by the same amount.

3.2. Prototyping your idea

3.2.1. What is prototyping?

3.2.1.1. Defining prototyping

Prototyping is the process of creating a rudimentary working model of a product or system. For prototyping in the IoT, it helps to have design skills, electrical skills, physical/mechanical skills (work with your hands to put things together), programming skills, and to understand how TCP/IP works. But you do not need to be an expert in any of these areas. In fact, prototyping helps you to refine these skills.

Because the IoT is still developing, there are still unknown tasks to discover. This is a great time to invent something that is part of the IoT. Because the IoT combines people, process, data, and things, there is no end to the inventions that the IoT can help create and then incorporate.

Prototyping

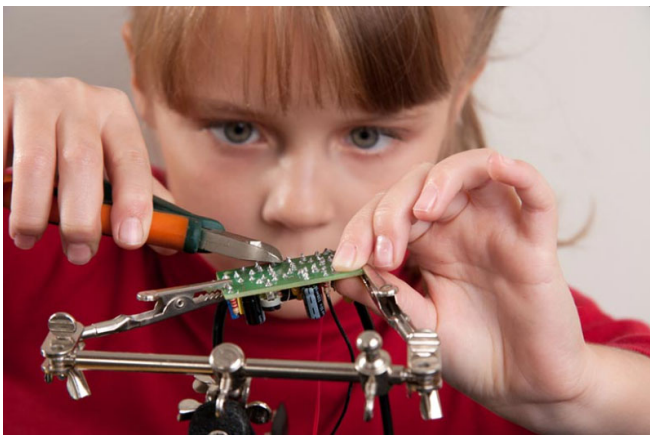
- Is fully functional, but not fault-proof.
- Is an actual, working version of the product.
- Is used for performance evaluation and further improvement of product.
- Has a complete interior and exterior.
- May be relatively expensive to produce.
- In the IoT, is often used as a technology demonstrator.

3.2.1.2. How to prototype?

How do you prototype? There are a few ways to get started. A team at Google used the "Rapid Prototyping Method" to create the Google Glass.
http://ed.ted.com/lessons/rapid-prototyping-google-glass-tom-chi to view a TedTalk about this process.

Of course, Google has a large number of resources to pay for the people and materials that go into prototyping. Most of us need some financial help to get our ideas out of our heads and into a prototype. For us, there is crowd funding. Kickstarter, Indiegogo, and Crowdfunder are just three of the many online crowd funding programs.

What IoT invention will you create?



3.2.2. Prototyping resources

3.2.2.1. Physical materials

A good place to start is, of course, the Internet. People have exchanged ideas for ages, but the Internet allows for idea exchanges on a whole new level. People who have never physically met can now collaborate and work together. There are several web sites you can visit to connect with other makers.

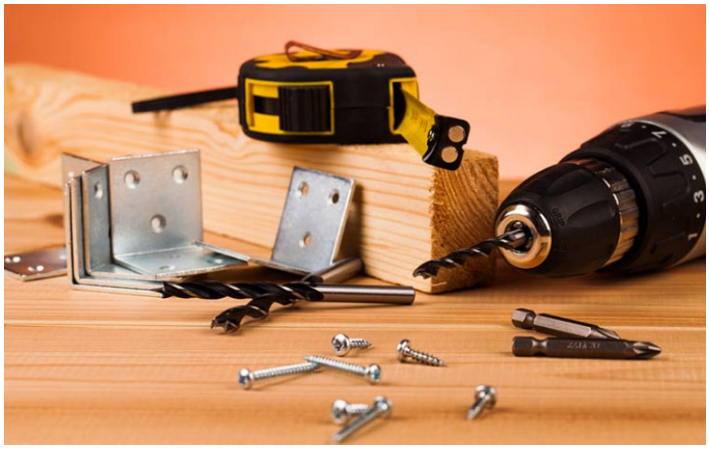
Maker Media is a global platform for connecting makers with each other to exchange projects and ideas. The platform also provides a place where makers can find and buy products for their projects. For more information, go to Makezine at http://makezine.com.

It is helpful to have practical skills when working with certain materials; for example, wood and metal are common prototyping materials, but they may be too difficult for a beginner to use. You might be surprised with what you can do with plastic, clay, paper, and wires. Search Google for more information or ideas on how to work with the different prototyping materials.

LEGO Mindstorms has a large community of contributors and fans. With LEGO Mindstorms, you can create LEGO robots and control them using an application. The kits come with everything you need to make it work. Go to LEGO Mindstorms at http://mindstorms.lego.com.

Meccano, or Erector Set, is a model construction system that consists of reusable metal strips, plates, angle girders, wheels, axles, and gears, with nuts and bolts to connect the pieces. It lets you build working prototypes and mechanical devices. Go to Erector Set at www.erector.us.

3D printing is the process of making a solid object based on a 3D model computer file. A machine, called a 3D printer, is connected to the computer. A number of companies now build and sell 3D printers. Go to Makerbot at https://www.makerbot.com.



3.2.2.2. Electronic toolkits

Computer programs cannot run without a computer. While you can create programs for almost any computer, some platforms are designed for the beginner. Below you will find some of the most popular platforms.

Arduino is an open-source physical computing platform based on a simple microcontroller board, and a development environment for writing software for the board. You can develop interactive objects that take input from a variety of switches or sensors to control lights, motors, and other physical objects. Go to Arduino at http://arduino.cc.

While the Arduino is not suitable for use as a computer, its low power requirement makes it capable of controlling other devices efficiently.

The Raspberry Pi is a low cost, credit-card-sized computer that plugs into a computer monitor or TV. You operate it using a standard keyboard and mouse. It is capable of doing everything a computer can do, from browsing the Internet and playing high-definition video, to making spreadsheets, word-processing, and playing games. Go to Raspberry Pi at http://www.raspberrypi.org.

The Beaglebone is very similar to the Raspberry Pi in size, power requirements, and application. The Beaglebone has more processing power than the Raspberry Pi; therefore, it is a better choice for applications with higher processing requirements. Go to Beaglebone at http://beagleboard.org.

3.2.2.3. Programing ressources

Programming is critical to the IoT. Creating custom code is very useful when developing an IoT solution. You have already learned about Blockly and Python. There are many other free resources that can help you develop your programming skills.

The MIT OpenCourseWare (OCW) is a web-based publication of almost all MIT course content. Open and available to the world, OCW is a great place to get familiar with computer programming for free. OCW programming related courses can be found at http://ocw.mit.edu/courses/intro-programming.

Khan Academy is a non-profit educational website created in 2006 to provide “a free, world-class education for anyone, anywhere”. The lectures related to computer programming can be found at https://www.khanacademy.org/computing/cs.

Code Academy is another excellent resource. It relies on interactivity to help people learn how to write computer programs. You can find them at http://www.codeacademy.com.

3.3. Summary

This chapter began by discussing how to apply basic programming to support IoT devices. Flowcharts are diagrams that are used to represent processes. There are two common types of computer software: system software and application software. Application software programs are created to accomplish a certain task. System software works between the computer hardware and the application program. Programming variables can be classified into two categories:

- **Local Variables** - These are variables that are within the scope of a program / function / procedure.
- **Global Variables** - These are variables that are in the scope for the time of the program's execution. They can be retrieved by any part of the program.
-

The most common logic structures are IF – THEN, FOR Loops, and WHILE Loops.
Blockly is a visual programming tool created to help beginners understand the concepts of programming. Blockly implements visual programming by assigning different programming structures to colored blocks. Python is a very popular language that is designed to be easy to read and write. Python is an interpreted language; therefore, an interpreter is required to parse and execute Python code. Variables are labeled memory areas that are used to store runtime program data. Python supports many useful functions and datatypes including Range(), Tuples, Lists, Sets, Dictionary. Python also implements two sub-structures named ELSE and ELIF.

Next, the chapter detailed prototyping. Prototyping is the process of creating a rudimentary working model of a product or system. A team at Google used the "Rapid Prototyping Method" to create the Google Glass. The Internet allows for idea exchanges on a whole new level. There are several web sites you can visit to connect with other makers.

4. Everything generate Data

4.1. Big Data

4.1.1. What is big data?

4.1.1.1. Introduction

Data is information that comes from a variety of sources, such as people, pictures, text, sensors, and web sites. Data also comes from technology devices like cell phones, computers, kiosks, tablets, and cash registers. Most recently, there has been a spike in the volume of data generated by sensors. Sensors are now installed in an ever growing number of locations and objects. These include security cameras, traffic lights, intelligent cars, thermometers, and even grape vines!

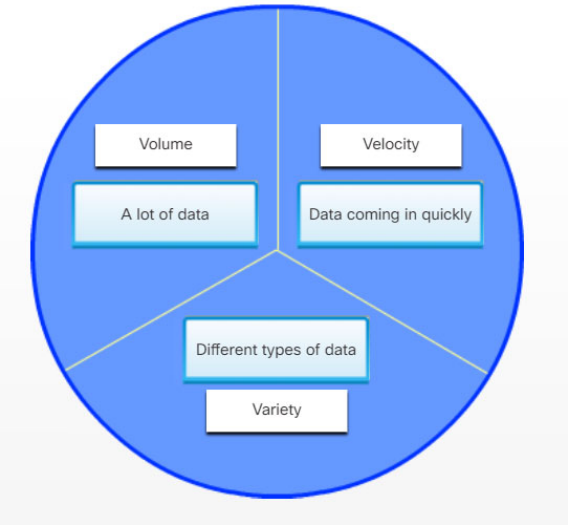
Big Data is a lot of data, but what is a lot? No one has an exact number that says when data from an organization is considered “Big Data.” Here are three characteristics that indicate an organization may be dealing with Big Data:

- They have a large amount of data that increasingly requires more storage space (volume).
- They have an amount of data that is growing exponentially fast (velocity).
- They have data that is generated in different formats (variety).

How much data do sensors collect? Here are some estimated examples:

- Sensors in one autonomous car can generate 4,000 gigabits (Gb) of data per day.
- An Airbus A380 Engine generates 1 petabyte (PB) of data on a flight from London to Singapore.
- Safety sensors in mining operations can generate up to 2,4 terabits (TB) of data every minute.
- Sensors in one smart connected home can produce as much as 1 gigabyte (GB) of information a week.

While Big Data does create challenges for organizations in terms of storage and analytics, it can also provide invaluable information to fine-tune operations and improve customer satisfaction.



4.1.1.2. Large Datasets

Companies do not necessarily have to generate their own Big Data. Smaller organizations might not have the sensors, the volume of customers, or the ability to generate the variety of information that could benefit their company. There are sources of free data sets available, ready to be used and analyzed by anyone willing to look for them.

Many companies of various sizes believe they have to collect their own data to see benefits from big data analytics, but it is simply not true.

4.1.2. Where is big data stored?

4.1.2.1. What are the challenges of big data?

IBM's Big Data estimates conclude that "each day we create 2.5 quintillion bytes of data". To put this into context, every minute of every day:

- We upload over 300 hours of YouTube video.
- We send over 3.5 million text messages.
- We stream over 86 thousand hours of Netflix video.
- We like over 4 million Facebook posts.
- We request over 14 million forecasts from The Weather Channel.

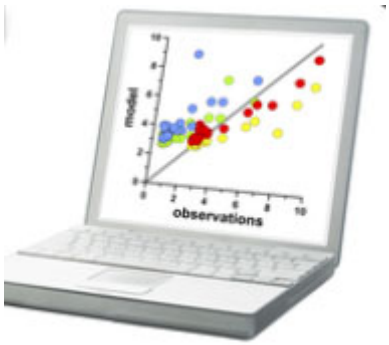
Go check : https://www.internetlivestats.com/

The rapid growth of data can be an advantage or an obstacle when it comes to achieving business goals. To be successful, enterprises must be able to easily access and manage their data assets.

With this enormous amount of data being constantly created, traditional technologies and data warehouses cannot keep up with storage needs. Even with the cloud storage facilities that are available from companies like Amazon, Google, Microsoft, and many others, the security of stored data becomes a big problem. Big Data solutions must be secure, have a high fault tolerance, and use replication to ensure data does not get lost. Big Data storage is not only about storing data, it is also about managing and securing it.

There are five major data storage problems with Big Data as represented in the figure.

- Management: Data can be generated and collected from multiple different sources so a management system must be used to organize and collate all of the sources. The are few data-sharing standards and thousands of data management tools available.



- Security: For data of value to enterprises, it must be kept secure and only accessible by authorized users.

- Redundancy: Safeguards should be in place to maintain the integrity of the stored data. Processes for backups, redundancy, and disaster recovery are required.

- Analytics: Big data contains both structured and unstructured data. Unstructured data,such as emails or photos, are difficult to analyze and consume a lot of storage space. Structured data, such as spreadsheet is easier to analyze and store. Data storage systems must be able to manage both types.

- Access: Big data must be accessible from anywhere at any time. Storage solutions need to support the quantity of input and output requests. Companies should also be aware of the strain placed on WAN links.

4.1.2.2. Where can be store big data ?

Big data is typically stored on multiple servers, usually housed within data centers. For security, accessibility, and redundancy, the data is usually distributed and/or replicated on many different servers in many different data centers.

Fog Computing

Fog computing is an architecture that utilizes end-user clients or “edge” devices to do a substantial amount of the pre-processing and storage required by an organization. Fog computing was designed to keep the data closer to the source for pre-processing.

Sensor data, in particular, can be pre-processed closer to where it was collected. The information gained from that pre-processed analysis can be fed back into the companies’ systems to modify processes if required. Because the sensor data is pre-processed by end devices within the company system, communications to and from the servers and devices would be quicker. This requires less bandwidth than constantly going out to the cloud.

After the data has been pre-processed, it is often shipped off for longer term storage, backup, or deeper analysis within the cloud.

4.1.2.3. The cloud and cloud computing

As mentioned before, the cloud is a collection of data centers or groups of connected servers. Access to software, storage, and services available on the servers is obtained through the Internet via a browser interface. Cloud services are provided by many large companies such as Google, Microsoft, and Apple. Cloud storage services are provided by different vendors such as: Google Drive, Apple iCloud, Microsoft OneDrive, and Dropbox.

From an individual's perspective, using the cloud services allows you:

- To store all of your data, such as pictures, music, movies, and emails, freeing up local hard drive space
- To access many applications instead of downloading them onto your local device
- To access your data and applications anywhere, anytime, and on any device

One of the disadvantages of using the cloud is that your data could fall into the wrong hands. Your data is at the mercy of the security robustness of your chosen cloud provider.

From the perspective of an enterprise, cloud services and computing support a variety of data management issues:

- It enables access to organizational data anywhere and at any time.
- It streamlines the IT operations of an organization by subscribing only to needed services.
- It eliminates or reduces the need for onsite IT equipment, maintenance, and management.
- It reduces the cost of equipment, energy, physical plant requirements, and personnel training needs.
- It enables rapid responses to increasing data volume requirements.

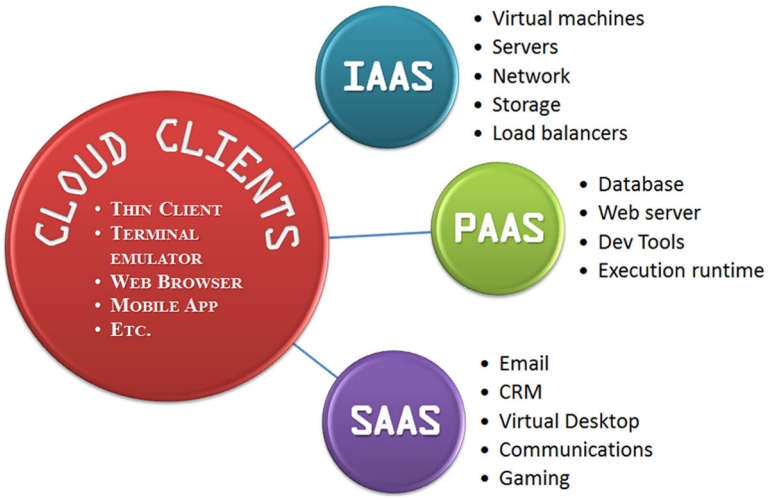
Cloud computing is another way to manage, store, and access data.

Cloud computing involves large numbers of computers connected through a network. Cloud computing providers rely heavily on virtualization to deliver their services. It can also reduce the operational costs by using resources more efficiently. These companies provide four distinct categories of services. Click the categories in the figure for more information.

Cloud computing allows the users to access their data anywhere and at any time. You are probably already using some form of Cloud computing if you use web-based email services.

Cloud computing also enables organizations to streamline their IT operations by subscribing only to needed services. By using Cloud computing, the organizations may also eliminate the need for onsite IT equipment, maintenance, and management. Cloud computing reduces costs for organizations. It reduces equipment costs, energy costs, physical plant requirements, and support personnel training needs.

- **SaaS:** Applications delivered over the web to the end users
- **PaaS:** Tools and services used to deliver the applications
- **IaaS:** Hardware and software to power servers, storage, networks and operating system
- **ITaaS:** IT professionals support applications, platforms and infrastructure



Types of cloud:

- Private
- Public
- Community
- Hybrid

- **A Private Cloud** is created exclusively for a single organization. The infrastructure could be physically located on or off site, and may be owned by a separate provider. The Private Cloud provides services only to members of the single organization.

- **A Public Cloud** is created for use by the general public. The infrastructure is physically located on the provider's site, but may be owned by one or multiple organizations that could include businesses, academic institutions, or governments.

- **A Community Cloud** is created for exclusive use by a specific community. The community consists of multiple organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). The infrastructure could be physically located on or off site, and may be owned by a separate provider or by one or more of the organizations in the community. The differences between public clouds and community clouds are the functional needs that have been customized for the community. For example, healthcare organizations must remain compliant with policies and laws (e.g., HIPAA) that require special authentication and confidentiality. Organizations can share the implementation effort of these requirements across a common cloud deployment.

- **A Hybrid Cloud infrastructure** is a composition of two or more distinct cloud infrastructures (private, community, or public) that are unique entities. These entities are bound together by technology that enables data and application portability. This portability allows an organization to maintain a single perspective of a cloud solution while taking advantage of the strengths available from different cloud providers. For example, geography (location to end users), bandwidth, policy or law requirements, security, and cost are all features that may differentiate providers. A Hybrid Cloud offers the flexibility to adjust and react to these provider services, on demand.

Data centers:

Data centers are a critical enabler of Cloud computing. A data center is a facility that provides the necessary services to host the largest computing environments in existence today. Its main function is to provide business continuity by keeping the computing services available at all times.

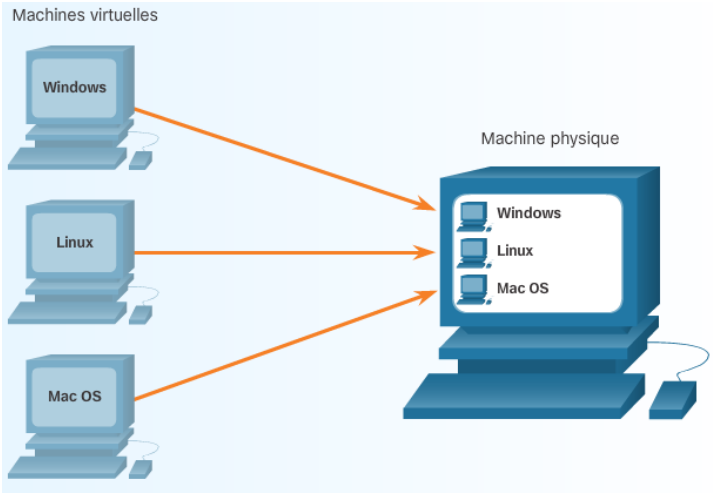
To provide the necessary level of service, several factors must be considered in a data center deployment:

- **Location**: Data centers should be located where there is reduced risk of natural disasters and sufficiently distanced from areas with high traffic of people (e.g. airports, malls, etc.) and areas of strategic importance to governments and utilities (e.g. refineries, dams, nuclear reactors, etc.)
- **Security**: A data center should extend tight controls over physical access and on-site personnel.
- **Electrical**: There should be sufficient access to electrical power. There should be backup power consisting of uninterruptible power supplies, battery banks, and electrical generators.
- **Environmental**: A tightly controlled physical environment that maintains appropriate temperature and humidity. It should also include sophisticated fire suppression systems.
- **Network** : The network infrastructure should be scalable and reliable with redundant connectivity.

Currently, there are over 3,000 data centers in the world that offer general hosting services (IaaS) to individuals and organizations. There are many more data centers that are owned and operated by private industries for their own use.

Virtualization

Historically, each computer has its own operating system, applications, and dedicated hardware components. Now, using software emulation, several virtual computers can run on a single physical computer. This means each virtual computer has its own operating system, applications, and dedicated hardware components. This is known as virtualization in computing. Each virtual machine, shown in the figure, operates independently.



In the corporate world, a single physical infrastructure can run multiple virtual infrastructures. By virtualizing the servers and networks, companies can reduce operational and administrative costs. The operational savings can come from the reduction in power and cooling requirements and the number of physical machines. A virtual server can be added to support additional applications.

You can also use virtualization for your personal computing needs. You can try a new operating system on your computer without damaging your current system. You can browse the Internet safely with your virtual machine. The virtual machine can be deleted if anything goes wrong.

4.1.2.4 Distributed processing

From a data management perspective, analytics were simple when only humans created data. The amount of data was manageable and relatively easy to sift through. However, with the explosion of business automation systems and the exponential growth of web applications and machine-generated data, analytics is becoming increasingly more difficult to manage. In fact, 90% of data that exists today has been generated in just the last two years. This increased volume within a short period of time is a property of exponential growth. This high volume of data is difficult to process and analyze within a reasonable amount of time.

Rather than large databases being processed by big and powerful mainframe computers and stored in giant disk arrays (vertical scaling), **distributed data processing** takes the large volume of data and breaks it into smaller pieces. These smaller data volumes are distributed in many locations to be processed by many computers with smaller processors. Each computer in the distributed architecture analyzes its part of the Big Data picture (horizontal scaling).

Most distributed file systems are designed to be invisible to client programs. The distributed file system locates files and moves data, but the users have no way of knowing that the files are distributed among many different servers or nodes. The users access these files as if they were local to their own computers. All users see the same view of the file system and are able to access data concurrently with other users.

Hadoop was created to deal with these Big Data volumes. The Hadoop project started with two facets: The Hadoop Distributed File System (HDFS) is a distributed, fault tolerant file system, and MapReduce, which is a distributed way to process data. Hadoop has now evolved into a very comprehensive ecosystem of software for Big Data management.

Hadoop is open-source software enabling the distributed processing of large data sets that can be terabytes in size and that are stored in clusters of computers. Hadoop is designed to scale up from single servers to thousands of machines, each offering local computation and storage. To make it more efficient, Hadoop can be installed and run on many VMs. These VMs can all work together in parallel to process and store the data.

Hadoop has two main features that have made it the industry standard for handling Big Data:

- Scalability - Larger cluster sizes improve performance and provide higher data processing capabilities. With Hadoop, cluster size can easily scale from a five node cluster to a one thousand node cluster without excessively increasing the administrative burden.

- Fault tolerance – Hadoop automatically replicates data across clusters to ensure data will not be lost. If a disk, node, or a whole rack fails, the data is safe.

4.1.3. Supporting businesses with big data

4.1.3.1. Why do businesses analyze data?

Every organization must become more efficient and innovative to stay competitive and relevant in the digitized world. The IoT is an integral part of achieving that efficiency and innovation.
The goal of many businesses is to collect and analyze the massive amounts of new product-usage data to gain valuable insights. Data analytics allows businesses to better understand the impact of their products and services, adjust their methods and goals, and provide their customers with better products faster. The ability to gain new insights from their data brings value to the business.

To businesses, data is the new oil. Like crude oil, it is valuable, but if it is unrefined it cannot be easily used. Crude oil has to be changed to gasoline, plastic, chemicals, and other substances to create a valuable product. It is the same with data. Data must be broken down and analyzed for it to have value.

Value comes from two primary types of processed data, transactional and analytical. Transactional information is captured and processed as events happen. Transactional information is used to analyze daily sales reports and production schedules to determine how much inventory to carry. Analytical information supports managerial analysis tasks like determining whether the organization should build a new manufacturing plant or hire additional sales personnel.

4.1.3.2. Source of information

The source of data in the large datasets is varied. Apart from sensor data, other data originates from anything that has been scanned, entered, and released to the Internet from sources such as:

- Social media sites - Facebook, YouTube, eHarmony, and Twitter
- HTTP, Web pages, and search engines on the Internet
- Historical data from public and private archives
- Metadata that is attached to emails, transmitted documents, and pictures
- Medical forms, insurance forms, and tax forms
- Genomics research using DNA

Collected data can be categorized as structured or unstructured.

Structured data is created by applications that use “fixed” format input such as spreadsheets or medical forms. Even if data is considered structured, different applications create files in different formats that are not necessarily compatible with one another. Structured data may need to be manipulated into a common format such as CSV.

Comma-separated values (CSV) files are a type of plaintext file that use commas to separate columns in a table of data, and the carriage return character to separate rows. Each row is a record. Although they are commonly used for importing and exporting in traditional databases and spreadsheets, there is no specific standard. JSON and XML are also plaintext file types that use a standard way of representing data records. These file formats are compatible with a wide range of applications. Converting data into a common format is a valuable way to combine data from different sources.

Unstructured data is generated in a “freeform” style such as audio, video, web pages, and tweets. Unstructured data requires different tools to prepare data for processing or analysis. The following are two examples:

- Web pages are created to provide data to humans, not machines. “Web scraping” tools automatically extract data from HTML pages. This is similar to a Web Crawler or spider of a search engine. It explores the web to extract data and create the database to respond to the search queries. Web scraping software may use Hypertext Transfer Protocol or a web browser to access the World Wide Web. Typically, web scraping is an automated process which uses a bot or web crawler to do data mining. Specific data is gathered and copied from the web to a database or spreadsheet. The data can then be easily analyzed.

- Many large web service providers such as Facebook provide standardized interfaces to collect the data automatically using application programming interfaces (APIs). The most common approach is to use RESTful APIs. RESTful APIs use HTTP as the communication protocol and JSON structure to encode the data. Internet websites like Google and Twitter gather large amounts of static and time series data. Knowledge of the APIs for these sites allow data analysts and engineers to access the large amounts of data that are constantly being generated on the Internet.

4.1.3.3. Data visualization

Data mining is the process of turning raw data into meaningful information by discovering patterns and relationships in large data sets.
To be of value, the mined data must be analyzed and presented to managers and decision makers. There are many different visualizations that can be used to present the value in the data. Determining the best chart to use will vary based on the following:

- Number of variables to show
- Number of data points in each variable
- Is the data representing a timeline
- Items that require comparisons
-

Some of the most popular chart types are line, column, bar, pie, and scatter.

4.1.3.4. Analyzing big data for effective use in business

Big data is just that – BIG! It is most useful if you can analyze it to get value out of it. Data analysis is the process of inspecting, cleaning, transforming, and modeling data to uncover useful information. Analyzing big data typically requires tools and applications created for this purpose. These analysis tools have been designed to provide businesses with detailed information, patterns, and valuable insights.

Before beginning any analysis, it is critical to know what problem the business is trying to solve or what information the business is looking for. Are they interested in customer behavior in specific states, energy consumption patterns in different city quadrants, or the number of Facebook "likes" based on age?

Having a strategy helps a business determine the type of analysis required and the best tool to do the analysis. A strategy also helps to determine the most effective way to present the results for management.

Tools and applications range from using an Excel spreadsheet or Google Analytics for small to medium data samples, to the applications dedicated to manipulating and analyzing really big datasets.

There are many Big Data Analytics tools that a business could select such as: Knime, OpenRefine, Orange, and RapidMiner.

- **Knime** : The KNIME analytics platform is the leading open solution for data-driven innovation, designed for discovering the potential hidden in data, mining for fresh insights, or predicting futures. Orgaizations can take their collaboration, productivity and performance to the next level with a robust range of commercial extensions to our open source platform.

- **OpenRefine** : Is a powerful tool for working with messy data. OpenRefine takes data and cleans it; transforming it from one format into another, and extending it with web services and external data. Please note that since October 2nd, 2012, Google is not actively supporting this project, which has now been rebranded to OpenRefine. Project development, documentation and promotion is now fully supported by volunteers.

- **Rapidminer** : Much like KNIM, Rapidminer operates through visual programming and is capable of manipulating, analyzing and modeling data. Rapidminer's unified data science platform accelerates the building of complete analytical workflows, from data prep to machine learning to model validation to deployment. This all happens in a single environment, dramatically improving efficiency and shortening the time to value for data science projects.

- **Orange** : Orange is open source data visualization and data analysis for novice and expert, and provides a large toolbox to create interactive workflows to analyze and visualize data. Orange is packed with different visualizations, from scatter plots, bar charts, trees, to dendrograms, networks and heat maps.

4.2.Summary

Big Data usually has three characteristics. It is a large amount of data that increasingly requires more storage space (volume), that is growing exponentially fast (velocity), and that is generated in different formats (variety).

Fog computing is an architecture that utilizes end-user clients or “edge” devices to do a substantial amount of the pre-processing and storage required by an organization. Fog computing was designed to keep the data closer to the source for pre-processing.

The cloud is a collection of data centers or groups of connected servers giving anywhere, anytime access to software, storage, and services using a browser interface. Cloud services provide increased data storage as required and reduce the need for onsite IT equipment, maintenance, and management. They also reduce the cost of equipment, energy, physical plant requirements, and personnel training needs.

Distributed data processing takes large volumes of data from a source and breaks it into smaller pieces. These smaller data volumes are distributed in many locations to be processed by many computers with smaller processors. Each computer in the distributed architecture analyzes its part of the Big Data picture.

Businesses gain value by collecting and analyzing massive amounts of new product-usage data to understand the impact of their products and services, adjust their methods and goals, and provide their customers with better products faster.

Collected data can be categorized as structured or unstructured. Structured data is created by applications that use “fixed” format input such as spreadsheets or medical forms. Unstructured data is generated in a “freeform” style such as audio, video, web pages, and tweets. Both forms of data need to be manipulated into a common format to be analyzed. CSV, JSON, and XML are plaintext file types that use a standard way of representing data records. Converting data into a common format is a valuable way to combine data from different sources.

Data mining is the process of turning raw data into meaningful information by discovering patterns and relationships in large data sets. Data visualization is the process of taking the analyzed data and using charts such as line, column, bar, pie, or scatter to present meaningful information. A strategy helps a business determine the type of analysis required and the best tool to do the analysis. A strategy also helps to determine the most effective way to present the results for management.

5.Everything can be automated

5.1. What can be automated?

5.1.1. Automation

5.1.1.1. What's automation?

Automation is any process that is self-driven and reduces, then eventually eliminates, the need for human intervention.

Automation was once confined to the manufacturing industry. Highly repetitive tasks such as automobile assembly were turned over to machines and the modern assembly line was born. Machines are excellent at repeating the same task without fatigue and without the errors that humans are prone to make in such jobs. This results in greater output, because machines can work 24 hours a day without breaks. Machines also provide a more uniform product.

The IoT opens up a new world in which tasks previously requiring human intervention can become automated. As we have seen, the IoT allows the collection of vast amounts of data that can be quickly analyzed to provide information that can help guide an event or process.

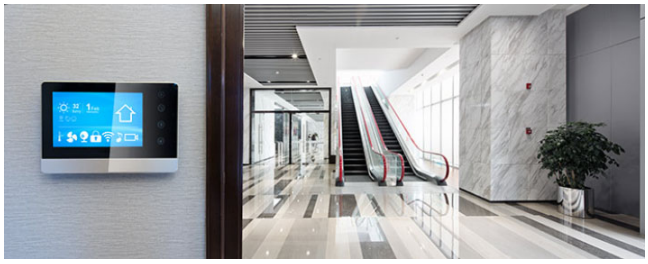
As we continue to embrace the benefits of the IoT, automation becomes increasingly important. Access to huge amounts of quickly processed sensor data started people thinking about how to apply the concepts of machine learning and automation to everyday tasks. Many routine tasks are being automated to improve their accuracy and efficiency.

Automation is often tied to the field of robotics. Robots are used in dangerous conditions such as mining, firefighting, and cleaning up industrial accidents, reducing the risk to humans. They are also used in such tasks as automated assembly lines.

We now see automation everywhere, from self-serve checkouts at stores and automatic building environmental controls, to autonomous cars and planes. How many automated systems do you encounter in a single day?

5.1.1.2. How is Automation being used?

- **Smart Home Automation:** For many, the home environment has become a more automated environment. Devices such as the Apple HomeKit, Amazon Alexa and Google assistant allow us to give voice commands to control such thing as lights, lock, doors, thermostats, plugs, switches, alarm systems, window coverings, sprinkler system sensors, and more… Even Kitchen appliances and pet care functions are being automated. Companies are producing new products every day to work with these home automation systems.

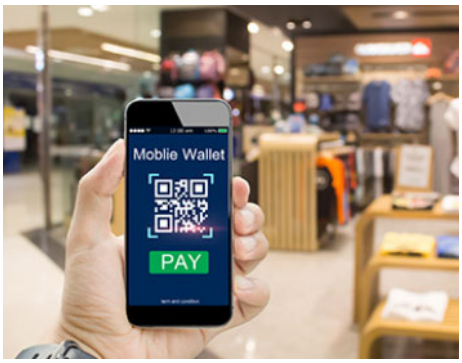


- **Smart buildings :** Enterprises of all types are using smart technology to automate building processes. Smart Buildings deploy many of the same technologies as smart homes. These processes provide efficient lighting, energy, heating, air conditioning, and security. For example, a smart building can reduce energy costs using sensors that detect how many occupants are in a room and adjust the heating or cooling appropriately. Smart buildings can also connect to and communicate with the smart grid. This enables more efficient management of energy systems.

- **Industrial Iot and Smart Factories :** The Industrial IoT(IIoT), brings together machines advanced analytics, and people. It is a network of manufacturing devices and sensors connected by secure, high-speed communications technologies. This results In systems that can monitor processes; collect, exchange, and analyze data; and use that information to continually adjust the manufacturing process.
We are currently in the fourth industrial revolution, or what is called Industry 4.0 . This describes an environment where machinery and equipment are able to improve processes through automation and self-optimization. Industry 4.0 extends beyond the manufacturing process and into functions like planning, supply chain logistics, and product development.

- **Smart Cities :** What do Hamburg Barcelona, Kansas City, Jaipur, Copenhagen and Manchester have in common ? They are all “smart cities” that use digital technology to make their city a better place to live. Some of these cities use technology to reduce carbon emissions or monitor C02 levels. Others use technology to provide free city-wide WI-FI access, improve public safety, or improve transportation options.

- **Smart cars technology :** Most of today’s new motor vehicles have integrated technology that assists drivers to be safer on the road. Technology exists that prevents drivers from drifting into adjacent lanes or making unsafe lane changes. Systems automatically apply the brakes if a vehicle ahead of them stops or slows suddenly. The safety technologies use a combination of hardware and software to identify safety risks and to take action to avoid a crash The continuing evolution of these technologies have given rise to ADS (Automated Driving Systems) that can handle the whole task of driving when we do not want to, or cannot do it ourselves. Self-driving vehicles can now operate fully autonomously, without the intervention of a driver.



- **Stores and Services:** Tasks that were once done by people are now increasingly being done by machines. Fast food restaurants are setting up self-serve kiosks for order entry, banks are increasingly turning to automated teller machines or apps that are designed to run on smart phone, and supermarkets and department stores have installed self-serve checkouts.
Systems have even been designed to monitor inventory levels and automatically place orders to accurately match supply to demand and eliminate excess inventory

- **Medical Diagnosis and Surgery:** The medical profession relies on doctors and nurses to run tests and make a diagnosis based on the results. Systems have now been developed that use technology to accurately and automatically conduct these medical tests. These systems then search through comprehensive data bases making a large number of calculations and comparisons. The result is in a more accurate diagnosis and treatment regime than might be possible from a single individual. Also, machines are now being used to more precisely control the treatment, which minimizes peripheral damage to the patient.

- **Aircraft auto-pilot:** Planes today are built to fly themselves. A complex collection of systems automates a plane's operations. After a flight path is entered, the autopilot system collects information about the route, location, air speed, altitude, and engine thrust. It makes adjustments keep the plane safety on the intended path. Redundancy in system design ensures that a failure in any on system would not jeopardize passenger safety.

5.1.1.3. When Things start to think

Can things think? Can a device learn from its environment? In this context, there are many definitions of the word "think". One possible definition is the ability to connect a series of related pieces of information together, and then use them to alter a course of action.

For example, when we are young we have no concept that a fire is hot and that placing our hand in the fire will cause pain. A fire may appear visually pleasing and actually encourage one to try and touch the flames. We quickly learn that the fire can cause injury. We then start to associate the image of the fire with the pain it can cause. From this point on we start to think about the results of touching the fire and base our actions on this acquired information.

Many devices now incorporate smart technology to alter their behavior under certain circumstances. This can be as simple as a smart appliance lowering its power consumption during periods of peak demand or as complicated as a self-driving car.

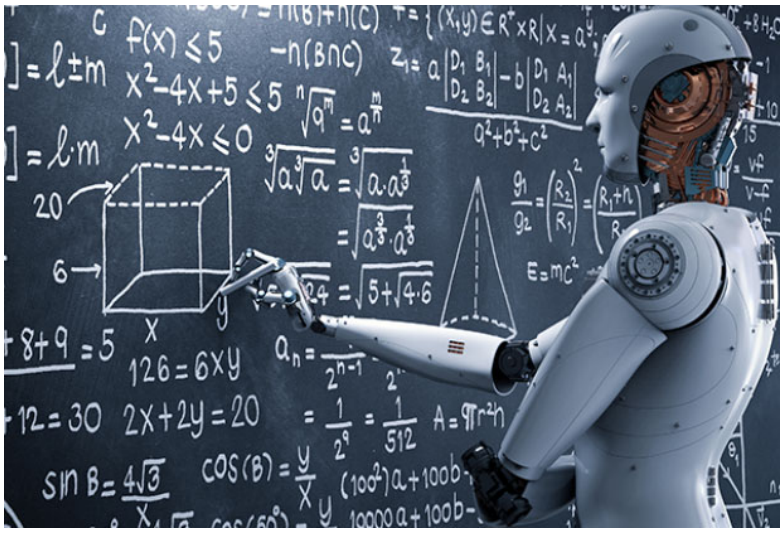
Whenever a decision or course of action is taken by a device based on an outside piece of information, then that device is referred to as a smart device. Many devices that we interact with now have the word smart in their names. This indicates that the device has the ability to alter its behavior depending on its environment. What smart technology and devices have you interacted with today?

	Automation	Not Automation
The temperature and lighting in your home or business is adjusted based on your daily routine.		
You use a remote device to start your car.		
You use online banking to pay a bill.		
Robots are used in dangerous conditions such as mining, firefighting, and cleaning up industrial accidents, reducing the safety risk to humans.		
Production levels are automatically tied to demand eliminating unneeded product and reducing the impact on the environment.		
You adjust the volume on the television set with a remote control.		
Your GPS recalculates the best route to a destination based on current traffic congestion.		
A refrigerator senses that you are out of milk and places an order for more.		

5.1.2. Artificial intelligence and machine learning

5.1.2.1. What is artificial intelligence and machine learning?

Artificial Intelligence (AI) is the intelligence demonstrated by machines. This is in contrast to natural intelligence which is the intelligence displayed by living organisms. AI uses intelligent agents that can perceive their environment and make decisions that maximize the probability of obtaining a specific goal or objective. AI refers to systems that mimic cognitive functions normally associated with human minds such as learning and problem solving.



Some of the tasks that currently are deemed to require a degree of AI are autonomous cars, intelligent routing in content delivery networks, strategic game playing, and military simulations.
As technology develops, many of the tasks that at one time required AI have become routine. Many of these tasks have migrated from AI to Machine Learning (ML).

ML is a subset of AI that uses statistical techniques to give computers the ability to “learn” from their environment. This enables computers to improve on a particular task without being specifically programmed for that task.

This is especially useful when designing and programming specific algorithms is difficult or infeasible. Examples of such tasks in computer science include malicious code detection, network intruder detection, optical character recognition, computer speech recognition, and computer vision.
One objective of learning is to be able to generalize based on experience. For machines, this involves the ability to perform accurately on new, previously unseen tasks after gaining experience with a learning data set. The training data set must come from data that is representative of the larger data pool. This data pool enables the machine to build a general model about this data, which would help it make accurate predictions.

5.1.2.2. ML in the IoT

One of the features of the IoT is that it enables the collection of extremely large pools of data that can "teach" programs how to respond in certain conditions. Some of the more common uses of ML technology include:

- **Speech Recognition** - Many different companies now offer digital assistants which allow you to use speech to communicate with a computer system. Apple, Microsoft, Google and Amazon all offer this service. These companies not only allow commands to be given verbally, but offer speech-to-text capabilities.

- **Product Recommendation** - Systems build up a customer profile and recommend products or services based on previous patterns. Users of Amazon and eBay receive recommendations on products. Organizations such as LinkedIn, Facebook, and GooglePlus recommend users you may wish to connect with.

- **Shape Recognition** - Programs exist that allow crude hand-drawn diagrams and notes to be converted to more formal diagrams and text. This allows the shapes and lines of hand writing to be converted to more formal text which can then be searched and analyzed.

- **Credit Card Fraud Detection** - A profile is constructed about the purchasing patterns of a client. Any deviation from these patterns triggers an alert and the system automatically takes action. This action ranges from denying the transaction to notifying the authorities. Some of the events that are detected and could indicate a fraudulent transaction include purchasing products not normally purchased, purchases in a different geographic area, rapidly purchasing many different products, and purchasing large-ticket items.

- **Facial Recognition** - Security cameras are everywhere, from stores and streets to airports and transportation hubs. These cameras continually scan the crowds, normally watching for dangerous or illegal activities, but they can also be used to identify and track individuals. The system builds a pattern of specific facial features and then watches for a match to these facial patterns triggering some action.

Think about your interactions with online and offline systems over the past week. How many ML applications have you interacted with?

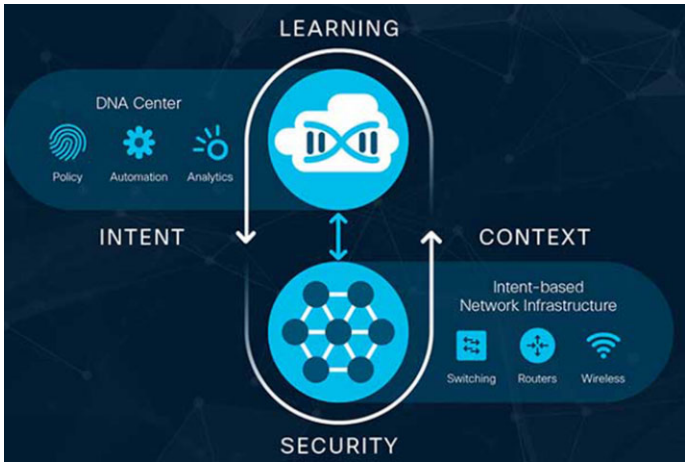
5.1.3. Intent-Based Networking

5.1.3.1. What is intent-based networking (IBN)

For a business to survive, it must be agile and respond quickly to the needs and demands of its customers. Businesses are increasingly dependent on their digital resources to meet customer demands, so the underlying IT network must also be responsive enough to quickly adapt to these requirements. This normally involves adjustments to many systems and processes. These adjustments may include changes to security policies and procedures, business services and applications, and operational policies.

With traditional networks, many different components must be manually adjusted to meet ever-changing business requirements. This requires different technicians and engineers to ensure that the systems are changed in a manner that allows them to work together to accomplish their goal. This sometimes results in errors and delays, and often in sub-optimal network performance.

The new business network must seamlessly and securely integrate IoT devices, cloud-based services, and remote offices in an agile, responsive, and business-relevant manner. Additionally, the network must secure these new digital initiatives from the ever-changing threat landscape.



To address this need, the IT industry has initiated an effort to create a systematic approach to tie infrastructure management to business intent. This approach is known as intent-based networking. The figure illustrates the general idea behind intent-based networking. With this new paradigm, business needs are automatically and continually translated into IT infrastructure execution.

5.1.3.2. How are Ml, AI and IBN linked?

Intent-based networking harnesses the power of automation, AI, and ML to control the function of a network to accomplish a specific purpose, or intent.

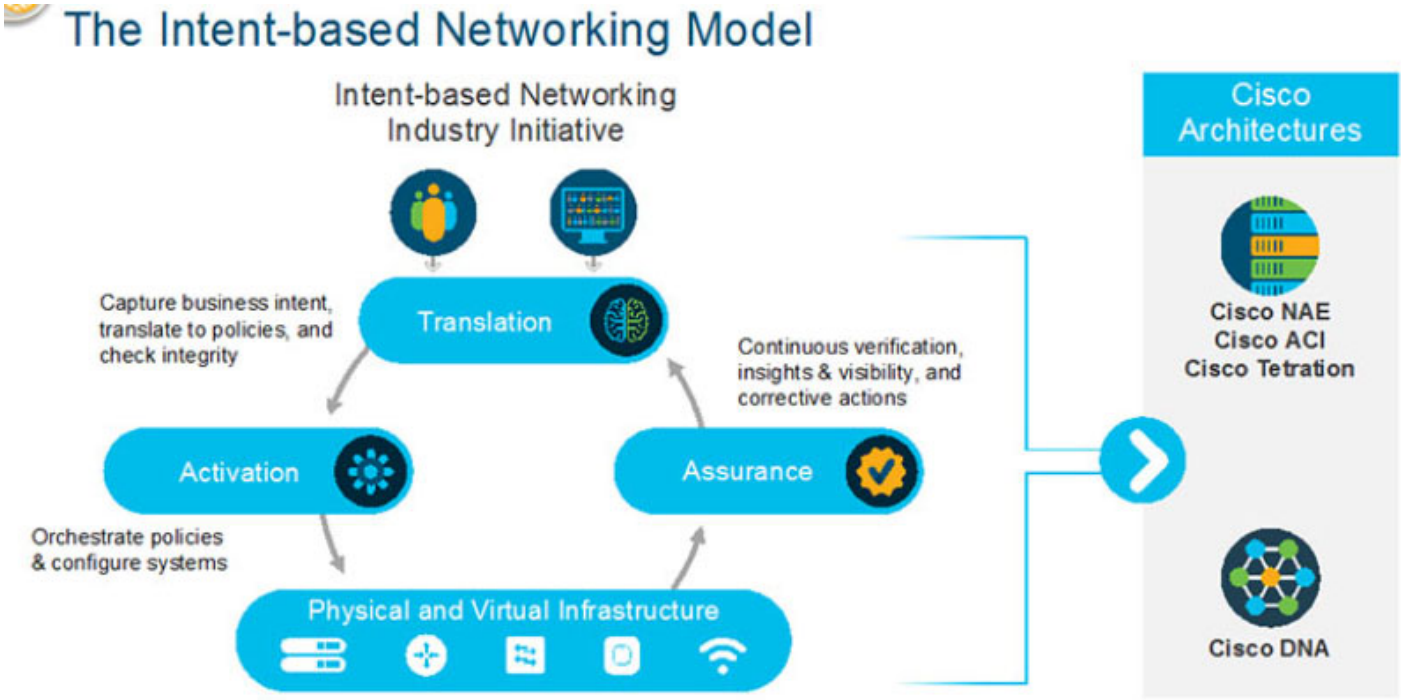
Intent-based networking allows the IT team to specify, in plain language, exactly what they want the network to accomplish and the network makes it happen. The network is able to translate the intent into policies and then use automation to deploy the appropriate configurations required across the network. The intent-based network uses AI and ML to ensure that any services that are deployed meet the required service level. If they do not meet the service level, the intent-based network can make alerts and provide suggestions for improvement. In some cases, the intent-based network can automatically reconfigure the network to comply with the service levels.

The intent-based networking model shown in the figure consists of three key elements:

- **Assurance** - The assurance element is end-to-end verification of network-wide behavior. It predicts the results of any changes, tracks compliance with the original intent, and makes recommendations or adjustments when there is a misalignment between the intent and the outcome. This stage relies heavily on AI and ML. Systems are part of a closed-loop that continually monitors performance and security of the network, and reconfigures the network to ensure compliance.

- **Translation** - The translation element is the ability to apply business intent to network configuration. The intent is what you wish to accomplish, not how it is accomplished. This intent is specified in plain language and used by the system to create policies across the system. For example, an intent might be to segment guest traffic from corporate traffic, or to enable access for remote users.

- **Activation** - The activation element occurs after the intent has been specified and the policies created. This is when individual devices are provisioned to match the intent-based policies. This can be an automated or semi-automated mode that allows the network team to verify configuration before the devices are deployed.



An intent-based network creates an agile, responsive network that scales easily and adapts to meet business requirements. It makes efficient use of highly-skilled resources and allows man and machine to work together to optimize the customer experience. Additionally, intent-based networking provides a more secure digital experience by automating time consuming or complicated processes. This makes deploying security policies much easier.

5.1.3.3. Use cases for intent-based networking

Intent-based networking allows the company to focus on business goals. It provides an automated system that understands what the organization needs and then makes it happen.

The Cisco Digital Network Architecture (Cisco DNA) is an example of an intent-based network. It is an open, extensible, software-driven architecture. It accelerates and simplifies enterprise network operations, while lowering costs and reducing risks.

Cisco DNA automation and assurance are built on a software-defined networking (SDN) controller, rich contextual analytics, network virtualization, and the limitless scalability of the cloud.

5.2. Summary

This chapter began by discussing automation. Automation is any process that is self-driven and reduces, then eventually eliminates, the need for human intervention. The IoT opens up a new world in which tasks previously requiring human intervention can become automated. Many devices now incorporate smart technology to alter their behavior under certain circumstances. Some examples of smart technology can be found in smart homes and buildings, cities, a smart power grid, and smart cars.

Next, the chapter detailed Artificial Intelligence (AI). AI is the intelligence demonstrated by machines. As technology develops, many of the tasks that at one time required AI have become routine. Many of these tasks have migrated from AI to Machine Learning (ML). ML is a subset of AI that uses statistical techniques to give computers the ability to “learn” from their environment. Some examples of ML in the IoT include speech and facial recognition, product recommendation, and credit card fraud detection.

The next topic of this chapter covered Intent-Based Networking (IBN). The new business network must integrate IoT devices, cloud-based services, and remote offices in a way that is relevant and responsive to business. The network must secure these new digital initiatives from the ever-changing threat landscape. IBN is a systematic approach to tie infrastructure management to business intent.

Finally, this chapter discussed how intent-based network uses AI and ML to ensure that any services that are deployed meet the required service level. A model of IBN contains three elements including assurance, translation and activation. The Cisco Digital Network Architecture (Cisco DNA) is an example of an intent-based network. It is an open, extensible, software-driven architecture.

6. Everything needs to be secured

6.1. Security in digitalized world

6.1.1. why is security so important?

6.1.1.1. Types of Data

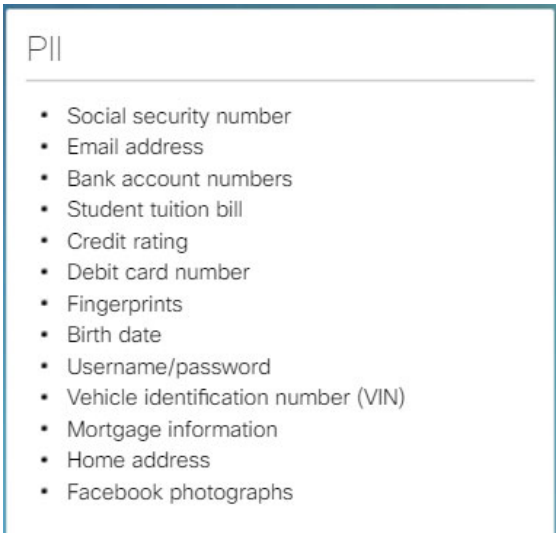
Has data really changed? Well technically no, data generated by computers and digital devices is still groups of 1s and 0s. That has not changed. What has changed is the quantity, volume, variety, and immediacy of the generated data.

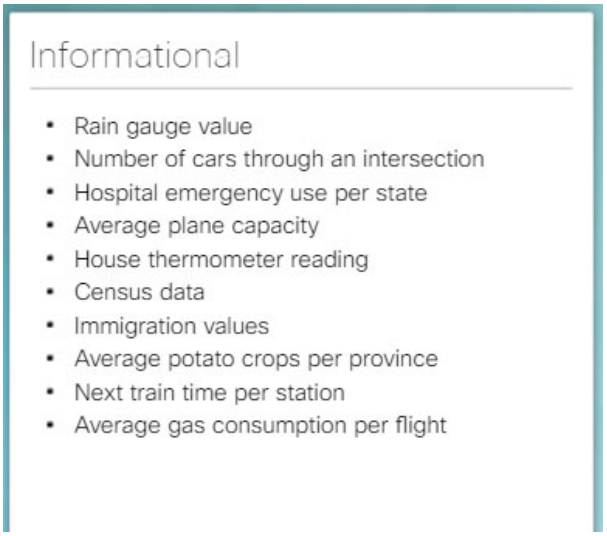
Historically companies would have access to our information gathered from forms, spreadsheets, applications, credit card purchases and other types of files. Much of the information was stored and analyzed at a later date. Sensitive data was still collected, stored and analyzed but, historically, hackers were more interested in hacking into systems to obtain corporate or government secrets.

Today, gathered data is taking on new characteristics. The digitized world has opened the floodgates for data gathering. IoT sensor-enabled devices are collecting more and more data of a personal nature. Wearable fitness trackers, home monitoring systems, security cameras, and debit card transactions are all collecting personal data as well as business and environmental data. Data is often combined from different sources and users may be unaware of this. 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.

Personally identifiable information (PII) or sensitive personal information (SPI) is any data relating to a living individual that can be used on its own or with other information to identify, contact, or locate a specific individual. The data gathered by companies and government institutions can also contain sensitive information concerning corporate secrets, new product patents, or national security.

Because we are gathering and storing exponential quantities of both sensitive and informational data, it has increased the need for extra security to protect this information from natural disasters, hackers, and misuse.





6.1.1.2. Who wants your data?

The Good Guys

Legitimate companies have an agreement in place that gives them permission to use the collected data about you for purposes of improving their business. Remember those "Terms and Conditions" or "Terms of Service and Agreements" documents that we say yes to but do not usually read? The next time that you are presented with one, take the time to read through it. The contents might surprise you.
Other legitimate users of our data would be companies that use sensors on their own devices or vehicles. Governments that have environmental sensors, and cities who have installed sensors on trains, busses or traffic lights also have a right to the data they generate.

Some hackers, called white hat hackers, are paid by legitimate companies and governments to test the security of a device or system. Their goal is not to steal or modify data but to help to protect it.

The Bad Guys

Other hackers, called black hat hackers, want access to collected data for many nefarious reasons:

- To sell the information to a third party.
- To modify the data or disable functionality on a device.
- To disrupt or to damage the image of a legitimate company.
- To access devices, web pages, and data to create political unrest or to make a political statement.
- To access user IDs and passwords to steal identities.
- To access data to commit a crime.
- To hack into systems to prove that they can do it.

6.1.1.3. Data in the wrong hands

- Hackers have accessed the data of many companies over the years. The impact is significant and has resulted in the data of millions of users being released on the web.

- According to recent news, login credentials and other personal data linked to more than one million yahoo and gmail accounts are reportedly being offered for sale on the dark web marketplace. The online accounts listed for sale on the Dark Web allegedly contain usernames, emails and plaintext passwords. The accounts are not from a single data breach; instead, several major cyber-attacks are believed to have been behind it.

- Cybercriminals penetrated Equifax (EFX), one of the largest credit bureaus, in July 2017 and stole the personal data of 145 million people. It was considered among the worst breaches of all time because of the amount of sensitive information exposed, including social security numbers. The company only revealed the hack two months later. It could have an impact for years because the stolen data could be used for identity theft.

- The breach in 2018 affected an estimated 150 million users of its food and nutrition application, MyFitnessPal. The investigation indicates that affected information may include usernames, email addresses, and hashed passwords.

- San Francisco (late 2016) – Uber disclosed Tuesday that hakers had stolen 57 million driver and rider accounts and that the company had kept the data breach secret for more than a year after paying a $100,000 ransom. The breach cost Uber in both reputation and money

Uber

- Anatomy of an IoT attack : https://cisco-netacad.wistia.com/medias/jjnqkypamu

6.1.2. Protecting the corporate web

6.1.2.1. Security best practices

Securing the network involves all of the protocols, technologies, devices, tools, and techniques that secure data and mitigate threats. Network security is largely driven by the effort to stay one step ahead of ill-intentioned hackers. Just as medical doctors attempt to prevent new illnesses while treating existing problems, network security professionals attempt to prevent potential attacks while minimizing the effects of real-time attacks. Networks are routinely under attack. It is common to read in the news about yet another network that has been compromised.

Security policies, procedures, and standards must be followed in the design of all aspects of the entire network. This should include the cables, data in transit, stored data, networking devices, and end devices.

Some security best practices:

- **Perform risk assessment:** Knowing the value of what ou are protecting will help in justifying security expenditures.
- **Create security policy:** Create a policy that clearly outlines company rules, job duties, and expectations
- **Physical security measures:** Restrict access to network assets in networking closets and server locations. Install appropriate fire suppression systems.
- **Human resource security measures:** Employees should be properly researched with background checks.
- **Perform and test backups:** Perform regular backups and test data recovery from backups
- **Maintain security patches and updates:** Regularly update server, and network device operating system and programs.
- **Employ access controls:** Configure user roles and privilege levels as well as strong user authentication.
- **Regularly test incident response:** Employ an incident response team and test emergency response scenarios
- **Implement a network monitoring, analytics and management tool**: Choose a security monitoring solution that integrates with other technologies.
- **Implement network security devices:** Use next generation routers, firewalls, and other security appliances.
- **Implement a comprehensive endpoint security solution:** use enterprise level antimalware and antivirus software.
- **Educate Users:** Educate users and employees in secure procedures.
- **Encrypt Data:** Encrypt all sensitive company data including

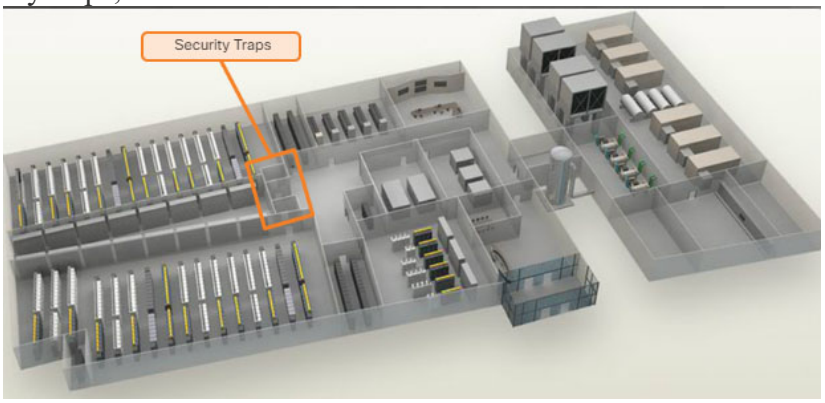
6.1.2.2. Physical security

Today's data centers store vast quantities of sensitive, business-critical information; therefore, physical security is an operational priority. Physical security not only protects access to the premises, but also protects people and equipment. For example, fire alarms, sprinklers, seismically-braced server racks, and redundant heating, ventilation, and air conditioning (HVAC) and UPS systems are in place to protect people and equipment.
Figure one shows a representation of a data center. List of elements:

- **Seismically-Braced server racks:** To protect people and equipment in case there is an earthquake.
- **On-premise security officers:** Monitor and enforce security policies.
- **Fences and gates:** Provide perimeter security to keep intruders out
- **Continuous video surveillance:** Provide real-time security monitoring
- **Electronic motion-detectors:** Provide inside security detections.
- **Security breach alarms:** Alarms generated in the facility controls center inform data center personnel of unauthorized physical access to the facility
- **Security traps:** Inside system to lock in intruder, also called mantrap
- **Biometrics access and exit sensors:** Provides two forms of authentication.
- **Gas-based fire suppression systems:** To protect people and equipment in case there is a fire
- **Redundant HVAC controlled environment:** To protect people and equipment in case the primary HVAC system goes down.
- **UPS backup:** To protect people and equipment during a power failure.

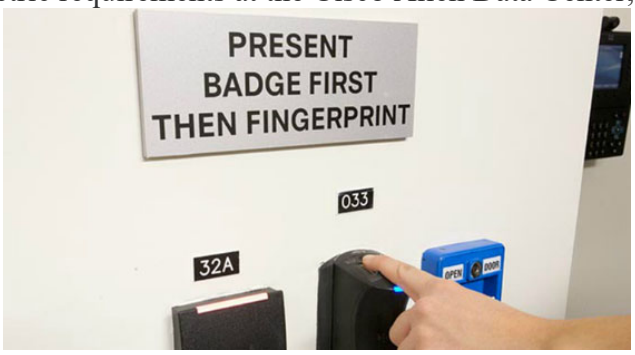
Physical security within the data center can be divided into two areas, outside and inside.

- **Outside perimeter security** - This can include on-premise security officers, fences, gates, continuous video surveillance, and security breach alarms.
- **Inside perimeter security** - This can include continuous video surveillance, electronic motion detectors, security traps, and biometric access and exit sensors.



Security traps provide access to the data halls where data center data is stored. As shown in Figure, security traps are similar to an air lock. A person must first enter the security trap using their badge ID proximity card. After the person is inside the security trap, facial recognition, fingerprints, or other biometric verifications are used to open the second door. The user must repeat the process to exit the data hall.

This figure displays the biometric requirements at the Cisco Allen Data Center, in Allen, Texas.



6.1.2.3. Challenges of securing IoT devices.

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. 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. The devices should be manufactured to be resistant to tampering, and they should be placed so that they are not obvious and are very difficult to access.

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.

Lack of Upgradeability - IoT sensor-enabled devices may be located in remote and/or inaccessible locations where human intervention or configuration is almost impossible. The devices are often designed to be in service many years longer than is typical for conventional high-tech equipment. 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, 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.

6.1.2.4. Safe Wi-fi usage

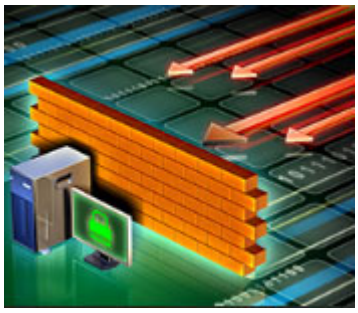
Wireless networks are popular in all types and sizes of businesses because they are easy to set up and convenient to use. For employees and guests, the company needs to deliver a wireless experience that enables mobility and security. If a wireless network is not properly secured, hackers within range can access it and infiltrate the network.

Steps to help protect your company wireless network:

- **Change the default administrator password:** Strong passwords should contain mora than 8 digits and consist of letters, numbers and special characters.
- **Change the network SSID:** A wireless network's name is called a service set identifier. Wireless routers are usually shipped with a default SSID making the network vulnerable to attack.
- **Do not advertise the SSID name:** Most Wireless routers advertise the SSID name. Employees would have knowledge of the SSID name through the company
- **Create a guest wirelles network:** For companies that require guest access, it is important to segregate the guest network from the employee network.
- **Enable the built in firewall:** Most wireless routers have built-in-firewall, but sometimes they ship with the firewall turned off. Make sure that the router's firewall is turned on.
- **Configure the wireless router to use WPA2-AES encryption:** Every wireless router offers encryption that scrambles your data and makes it unreadable to everyone except by the intended recipient. Wi-fi protected access 2 (WPA2) is best because it employs the hardest-totcrack encryption algorithm.

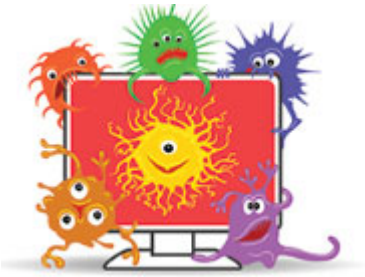
- **Keep the wireles router's firmware updated**: When you keep your wireless router's firmware updated, known bugs and vulnerabilities are fixed, making your router more secure.
- **Use MAC adress filtering**: If only employees use a particular wireless network, configure your wireless router to check the MAC addresses of devices trying to connect to it, allowing connections only from the devices it recognizes.
- **Disable wireless router's remote management feature**: Many wireless routers have a feature that lets you manage them from a remote location. Unfortunately, it often leaves routers susceptible to attacks. Disable remote management if you do not need to use this feature.
- **Physically secure the wireless router**: Ensure that the router is in a secure location and is only accessible by authorized personnel.

6.1.2.5. Protecting Devices



- **Keep the firewall on:** Whether it is a software firewall or a hardware firewall on a router, the firewall should be turned on and updated to prevent hackers from accessing your personal or company data.

- **Manage your operating system and browser:** Hackers are always trying to take advantage of vulnerabilities in your operating systems and your web browsers. To protect your computer and your data, set the security setting on your computer and your browser at medium or higher. Update your computer's operating system including your web browsers and regularly download and install the latest software patches and security updates from the vendors.



- **Use antivirus and antispyware:** Malicious software, such as viruses, Trojan horses, worms, ransomware and spyware, are installed on your computing devices without your permission, in order to gain access to your computer and your data. Viruses can destroy your data, slow down your computer, or take over your computer. Only download software from trusted websites to avoid getting viruses and spyware in the first place. Antivirus software is designed to scan your computer and incoming email for viruses and delete them. Sometimes antivirus software also includes antispyware. Keep your software up to protect your computer from the newest malicious software.

- **Protect all your devices:** Your computing devices, whether they are routers, PCs, laptops, tablets, or smartphones, should be password protected to prevent unauthorized access. The stored information should be encrypted, especially for sensitive or confidential data. For mobile devices, only store necessary information, in case these devices are stolen or lost when you are away from your home. If any one of your devices is compromised, the criminals may have access to all your data through your cloud-storage service provider, such as Icloud or Google drive.

6.1.3 Securing personal data and devices

6.1.3.1. Smart homes

Smart home technology has become very popular and its popularity is increasing every year as the technology evolves. Who doesn't find it appealing to turn your home thermostat up or down while you are at work, or to have your refrigerator order groceries to be delivered when you get home? How cool is it to check on the dog or to verify that your teenagers are doing their homework after school by activating your home security cameras?

As we install more and more smart sensors into our homes, we do increase the potential for security issues. Often the sensors are connected to the same network as our home or small business devices so that a breach of one device can radiate outwards to affect all connected devices. The sensors could also provide a way for hackers to get into our home network and gain access to any PCs and data that are connected to it.
Even virtual assistants such as Apple SIRI, Amazon Echo, or Google Home can be security risks. People use these devices to turn on music, adjust room temperatures, order products on-line, and get directions for where they are going. Can this cause any harm? It is possible that personal information such as passwords or credit card information could be leaked.

Fortunately many of the security flaws of the early smart technology sensors have already been discovered. Developers are working to correct the flaws and improve security measures to protect their systems from attack. Before purchasing home security systems, it is very important to research the developer and the security and encryption protocols that are in place for its products.

6.1.3.2. Public hotspots

When you are away from home, a public Wi-Fi hot spot allows you to access your online information and surf the Internet. Common activities on public Wi-Fi include logging into a personal email account, entering personally identifiable information, logging into social media, and accessing bank or financial information. All of this information could be stolen if the Wi-Fi connection is unsecure.

Safety rules to follow if you are using a public or unsecure Wi-Fi hotspot:

- Do not access or send any sensitive personal information over a public wireless network.
- Verify whether your computer is configured with file and media sharing, and that it requires user authentication with encryption.
- Use encrypted virtual private network (VPN) tunnels and services. The VPN service provides you secure access to the Internet, with an encrypted connection between your computer and the VPN service provider's VPN server. With an encrypted VPN tunnel, even if a data transmission is intercepted, it is not decipherable.

Many mobile devices, such as smartphones and tablets, come with the Bluetooth wireless protocol. This capability allows Bluetooth-enabled devices to connect to each other and share information. Unfortunately, Bluetooth can be exploited by hackers to eavesdrop on some devices, establish remote access controls, distribute malware, and drain batteries. To avoid these issues, keep Bluetooth turned off when you are not using it.

6.1.3.3. Setting up a VPN on Smartphones

A VPN is a secure network using an encrypted Internet connection that acts as a secure "tunnel" for data. It can be created over the public Internet connection to enable users to hide their identity when they are using the Internet. You should use a VPN service when you connect to a Wi-Fi network that is not your own (e.g. at the library or coffee shop). It prevents others on that public network from eavesdropping on your web use when you are using non-secure websites or communications.

Many businesses require VPN access into their internal networks if employees are working remotely or are mobile. The employee will be provided with the VPN client, as well as user ID and password information. For those who do not have access to a business VPN, there are many smartphone VPN service applications that you can download for free or for a monthly fee. Examples of these VPN apps include: ExpressVPN, NordVPN, and TunnelBear.

If you have a business VPN or if you download a VPN service application, they will provide the information and support required to set up your VPN.

How to manually set up a VPN from the Android settings

Step 1 • Unlock your phone.
Step 2 • Open the **Settings** app.
Step 3 • Under the **Wireless & networks** section, select **More**.
Step 4 • Select **VPN**.
Step 5 • At the top-right corner you will find a plus sign (+), tap it.
Step 6 • Your network administrator will provide you with all your VPN information.Simply select your desired protocol and 'enter all the information.
Step 7 • Tap **Save**.
Step 8 • You can connect by going back to the VPN settings and selecting your VPN of choice. You will be asked to enter a username and password.
Step 9 •You can also hit the 3-dot menu button to set your VPN to always be on.

How to manually set up a VPN on your iPhone or iPad

Step 1 • Launch **Settings** from your Home screen.
Step 2 • Tap **General**.
Step 3 • Tap **VPN**.
Step 4 • Tap **Add VPN Configuration**. If you have one already configured, select the **VPN client** you want to use and toggle the **Status** switch on.
Step 5 • Tap **Type**.
Step 6 • Select your **VPN type** from IKEv2, IPsec, or L2TP
Step 7 • Tap **Add Configuration** in the upper left corner to go back to the previous screen.
Step 8 • Enter the **VPN settings information** including description, server, and remote ID
Step 9 • Enter your **authentication login** including your username (or certificate), and password.
Step 10 • If you use a proxy, enable it by tapping **Manual** or **Auto**, depending on your preferences.
Step 11 • Tap **Done**.
Step 12 • Under VPN Configurations, toggle the **Status** switch on.

6.2. Summary

This chapter began by discussing the types of data. Personally identifiable information (PII) or sensitive personal information (SPI) is any data relating to a living individual that can be used on its own or with other information to identify, contact, or locate a specific individual. Legitimate companies have an agreements (Terms and Conditions or Terms of Service) that gives them permission to use the collected data about you for purposes of improving their business. Other legitimate users of our data would be companies that use sensors on their own devices or vehicles. Governments that have environmental sensors, and cities who have installed sensors on trains, busses or traffic lights also have a right to the data they generate.

Some hackers, called white hat hackers, are paid by legitimate companies and governments to test the security of a device or system. Their goal is not to steal or modify data but to help to protect it. Black hat hackers want access to collected data for many reasons, including selling it, damaging the reputation of a person or company, and causing political unrest.

Next, the chapter detailed security best practices. Security includes physically securing the outside and inside perimeters of places, such as data centers, where data is stored. Securing IoT devices is challenging due to the sheer number of them, the fact that they are found in non-traditional locations, and that many of them cannot be upgraded.

Black hat hackers frequently access available Wi-Fi. There are many steps you can take to protect your company's wireless network. To protect devices, keeps the firewall turned on, manage your operating system and browser, and use antivirus and antispyware.

Safety rules to follow if you are using a public or unsecure Wi-Fi hotspot:

- Do not access or send any sensitive personal information over a public wireless network.
- Verify whether your computer is configured with file and media sharing, and that it requires user authentication with encryption.
- Use encrypted virtual private network (VPN) tunnels and services. The VPN service provides you secure access to the Internet, with an encrypted connection between your computer and the VPN service provider's VPN server. With an encrypted VPN tunnel, even if a data transmission is intercepted, it is not decipherable.

As we install more and more smart sensors into our homes, we do increase the potential for security issues. Often the sensors are connected to the same network as our home or small business devices so that a breach of one device can radiate outwards to affect all connected devices.

7. Complement

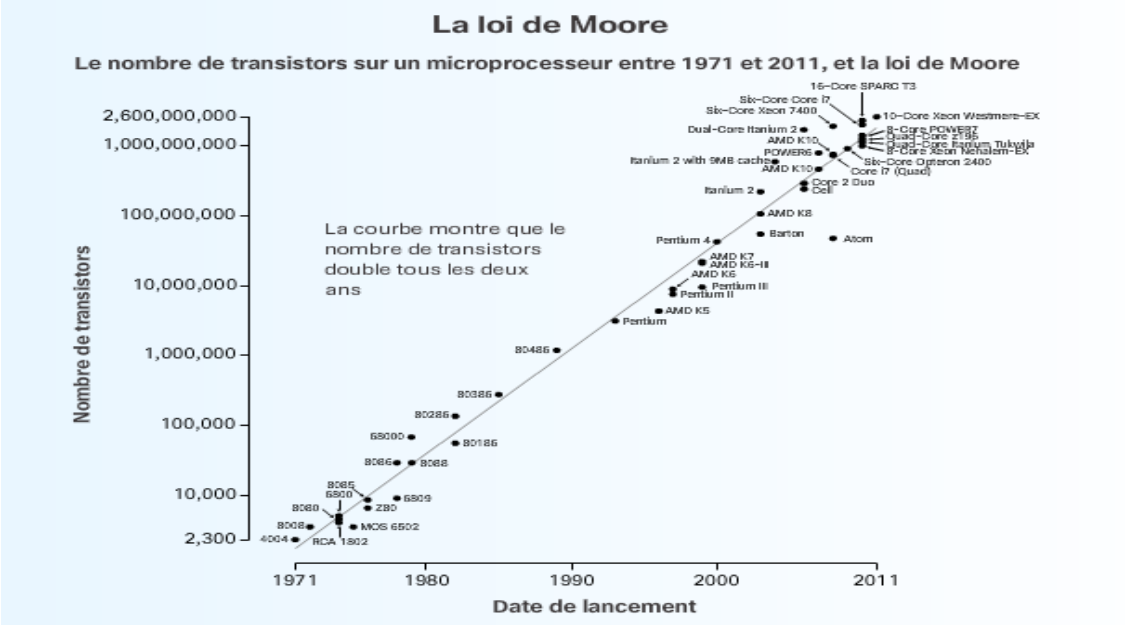
7.1. The laws

7.1.1. Technological growth

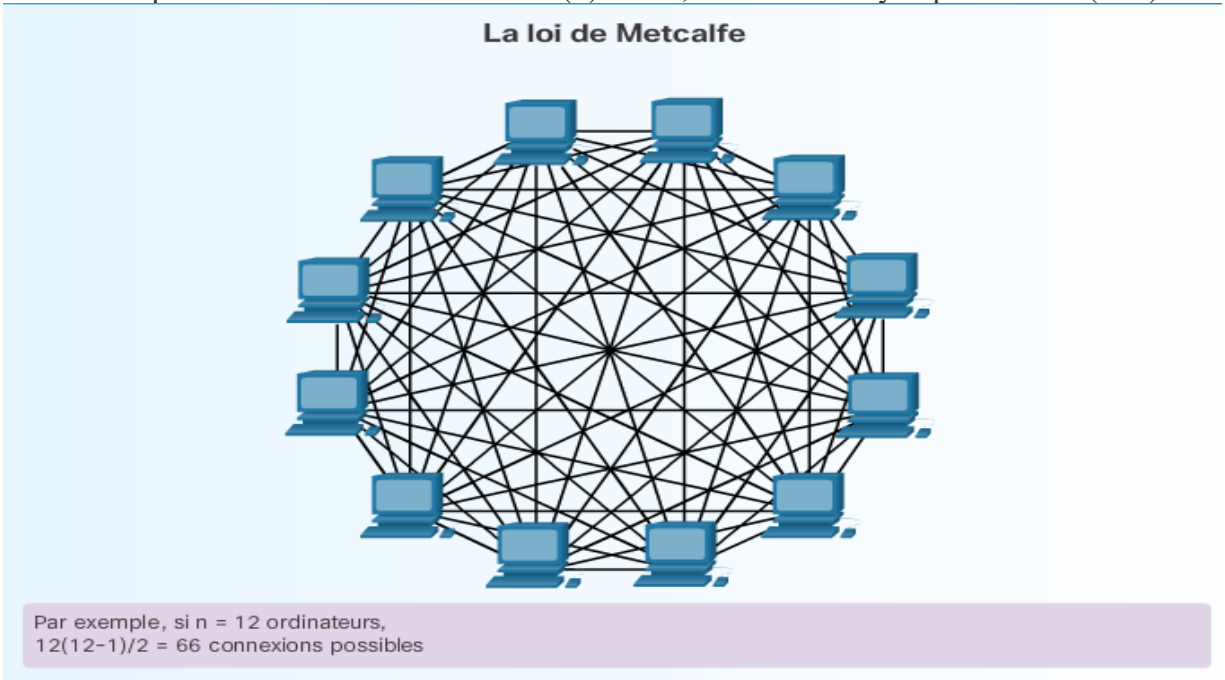
Today, the rate of technological growth is accelerating exponentially. To maintain a competitive advantage, organizations must be able to account for this growth.

There are three primary principles, referred to as laws that organizations and experts can use to help them plan for technological needs:

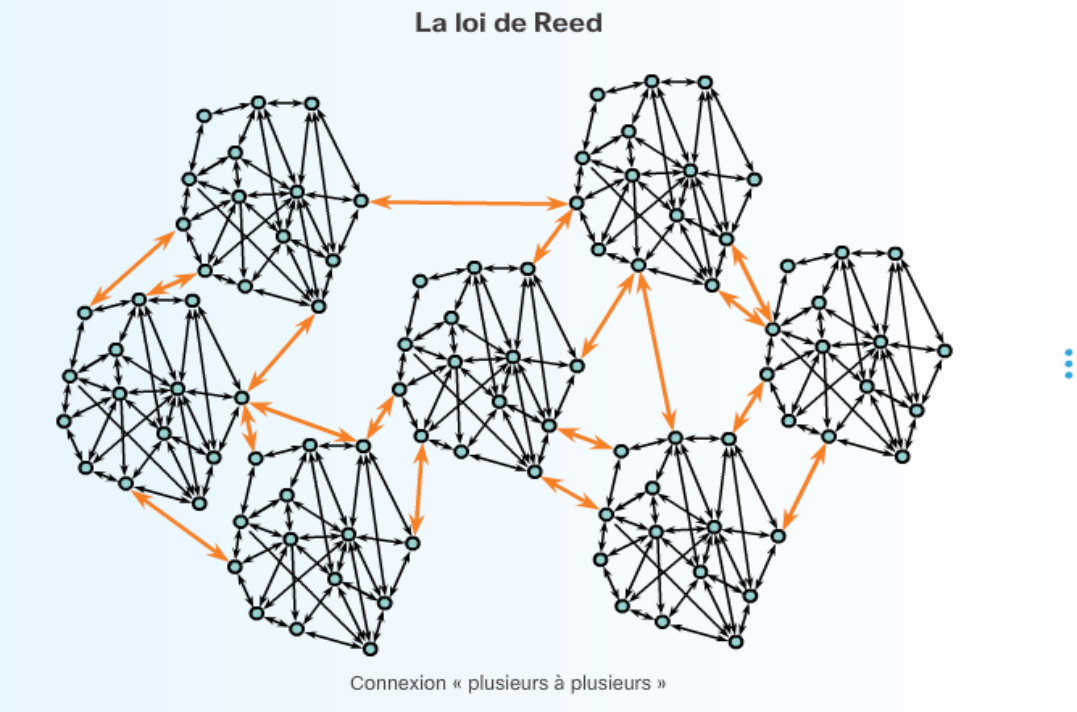
- **Moore's law:** This law was proposed by Gordon E. Moore, co-founder of Intel, in 1965. It states that the number of transistors on integrated circuits tend to double every two years, which increases processing capacity.



- **Metcalfe's law :** This law is attributed to Robert Metcalfe. It states that the value of a given network is proportional to the square of the number of users connected to it. Metcalfe's Law relates to the number of unique connections in a network of (n) nodes, mathematically expressed as n(n−1)/2



- **Reed's Law:** This law was proposed by David Reed. It states that the value of the network grows exponentially if you add up all the potential two-person groups, three-person groups, etcetera, that members could form.



Metcalfe's law is frequently mentioned when explaining the Internet's explosive growth. Together, Metcalfe's and Moore's laws provide a solid foundation to explain the ever-increasing presence and value of information technology in people's daily lives.

7.1.2. The IoE architectural approach

Cisco's architectural approach to the IoE is organized into three functional layers. The application layer is dependent on the platform layer, which is dependent on the infrastructure layer. Click each layer in the figure for more information on its role in the IoE architectural approach.

This architectural approach reflects the service models of the Cloud Computing model, taking advantage of Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS).

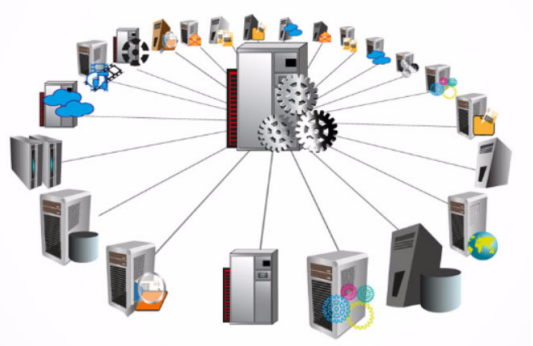
Application Layer	This Layer provides automated, dynamic, application-centric responses to changing traffic and usage demands. The application layer includes the intelligence needed to improve use experiences. It allows for the integration of traditional IT apps, and the use of collaboration applications and industry specific appliation.
Platform layer	This refers to Cisco solutions that provide orchestration, management, and policy adjustments based on changing demands, to accelerate service delivery. It allows applications and users to receive the resources they need, when they need them, without manual or coplicated IT tasks and configuration changes. The platform layer creates business agility by implementing new services and new analytical applications that can handle Big Data needs.
Infrastructure layer	This layer integrates power, security, core networls, access architectres, and storage with physical and virtual resources. It includes the right mix of hardware and software Across enterprse, cloud, and service provider networks. It converges all connections, Both OT and IT, into IP and accounts for cloud computing and mobile connectivity.

7.1.3. Data storage

Three primary types of data storage:

- **Local data :** Refers to data that is accessed directly, by local devices. Hard disks, USB flash drives, and optical disks are examples of local data storage.

- **Centralized data** : Data that is stored and shared from a single centralized server. This information can be accessed remotely by multiple devices over the network or the Internet. Using a centralized data server can result in bottlenecks and inefficiencies, and can become a single point of failure.



- **Distributed data** : Data that is managed by a distributed database management system (DDBMS). Distributed data is data that is replicated and stored in multiple locations. This allows for easy and efficient sharing of data. Distributed data is accessed through the use of local and global applications. With a distributed system, there is no single source of failure. Should one site lose power, users are still able to access data stored at the other sites.