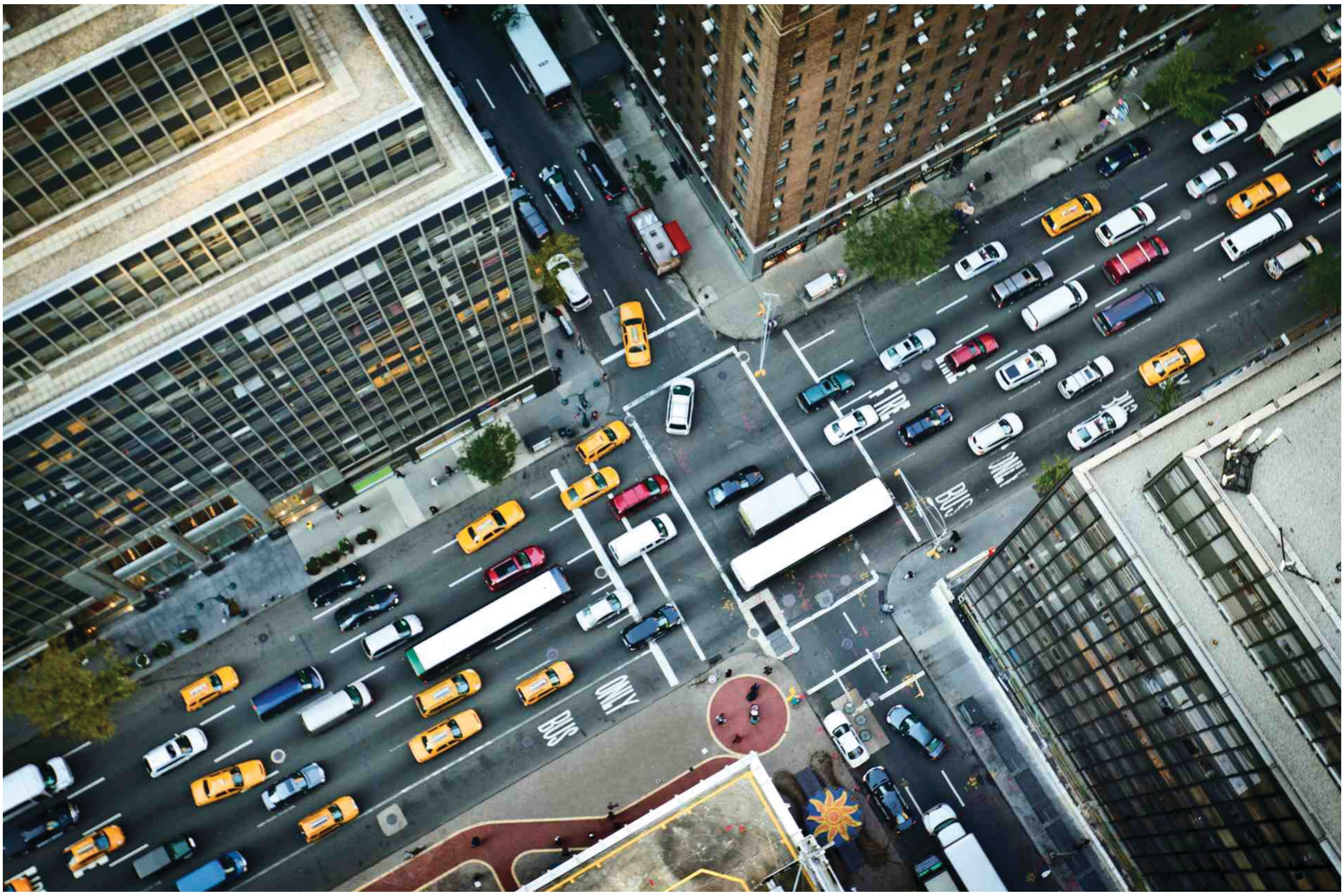
Internet of everything



About this free course

This free course is an adapted extract from the Cisco Networking Academy course IoE *Internet of everything*: .

This version of the content may include video, images and interactive content that may not be optimised for your device.

You can experience this free course as it was originally designed on OpenLearn, the home of free learning from The Open University - www.open.edu/openlearn/science-maths-technology/internet-everything/content-section-overview

There you'll also be able to track your progress via your activity record, which you can use to demonstrate your learning.

Intellectual property

Contents

Introduction

Early in your reading you will discover that the terms 'internet of everything' and 'internet of things' are interchangeable. Many British readers will be used to the different words being used for the same thing. In our living rooms, we can equally sit on a sofa or a settee. There is no difference between the two, we are sitting on the same thing.

This is the same for the internet of everything (IoE) and the internet of things. The IoE is an evolving idea, at its simplest level, we are using the internet to communicate with multiple distributed devices. In the hope that it will make our lives easier, offer new opportunities and extend the human experience. As you read this course, you will discover some of the ideas already explored with IoE as well as begin to formulate your own view how IoE could be a game changer. From smart homes to smart cities and agile manufacturing, IoE offers us some interesting opportunities.

A note about spellings: While The Open University is a UK organisation, Cisco, who originally developed this course, are based in the USA. Therefore you may notice that some of the images contain the original American spellings.

This free course, *Internet of everything*, presents introductory material and is intended to be easily accessible for those with some basic knowledge of computer systems and how they operate.

When you have read this chapter, you will have explored:

- the sheer scale of the internet
- how the physical world can connect to the internet
- how the internet has already changed our lives
- where we (the people) fit in with the evolving internet
- where we (the people) fit in with the evolving internet.

Before you start, The Open University would really appreciate a few minutes of your time to tell us about yourself and your expectations of the course. Your input will help to further improve the online learning experience. If you’d like to help, and if you haven't done so already, please fill in this optional survey.

Contents

Session 1: What is the IoE?

1.1 Internet of everything

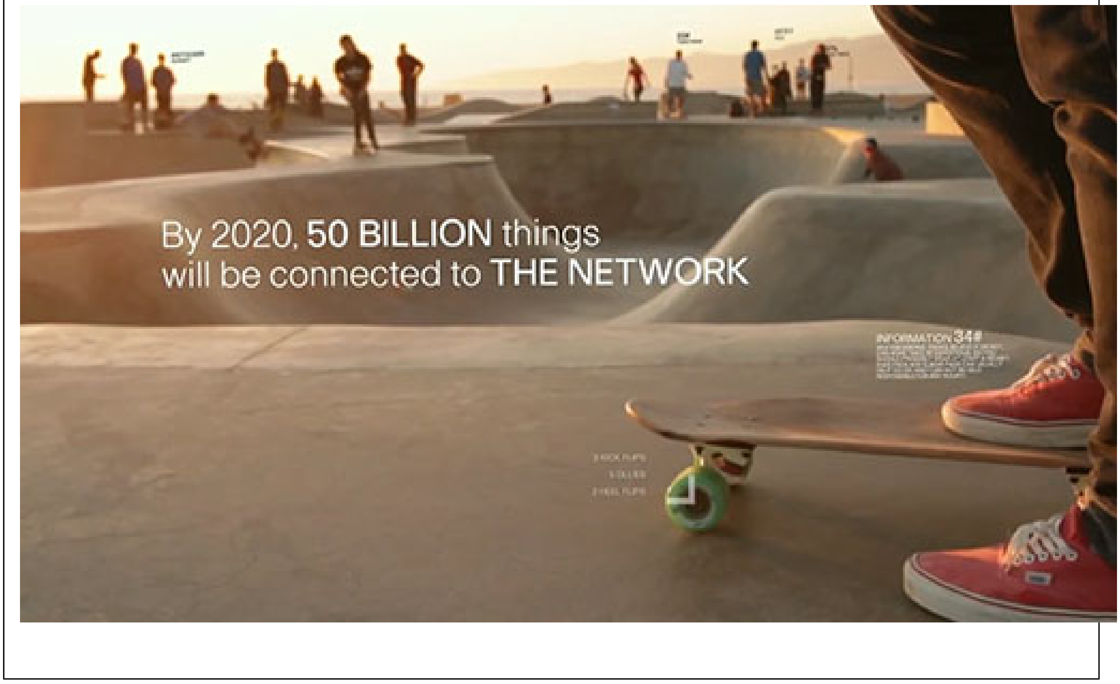
In the first session of the *Internet of everything* we will introduce you to the internet and how it is evolving into the IoE. The internet has evolved in ways that we could never have imagined. In the beginning, advancements occurred slowly. Today, innovation and communication are happening at a remarkable rate.

Think back 5, 10, 15 years and consider how you and maybe others around you used the internet. What has been a game changer in their lives as well as your own?

From its humble beginning as the Advanced Research Projects Agency Network (ARPANET) in 1969, where 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 take a glimpse into the future!

Video content is not available in this format.



1.1.1 Evolution of the internet

You may not have realised that the evolution of the internet has witnessed four distinct phases. Each phase has a more profound effect on business and society than the phase before. This course offers a combination of phases one, two and three to simply explain phase four.

Table 1 Four phases of the internet

Phase 1	Phase 2	Phase 3	Phase 4
Connectivity	Networked economy	Collaborative experiences	Internet of everything
Digitise access to information	Digitise business process	Digitise interactions (business and social)	Digitise the world, connecting
• email • web browser • search	• e-commerce • digital supply chain • collaboration	• social • mobility • cloud • video	• people • process • data • things
The first phase started over 20 years ago and is referred to as 'connectivity'. Email, web browsing and searching for content was just beginning.	The second phase started in the late 1990s and was the 'networked economy' phase. This was the birth of e-commerce and digitally connected supply chains. It changed the way we shopped and how companies reached new markets.	The third phase started in the early 2000s and is known as the 'collaborative experiences' phase. This phase is dominated by widespread use of social media, mobility, video, and Cloud computing. This phase completely transformed the world of work.	The current phase is called the 'internet of everything (IoE)'. This phase connects people, processes, data, and things, turning information into actions that create new capabilities, richer experiences, and unprecedented opportunities.

1.1.2 Cisco's intelligent network

As a technological society, we are entering the fourth phase of the internet, which we call the internet of everything (IoE). Cisco’s intelligent network works at the centre of the IoE.

Cisco has been finding new ways to communicate and collaborate for years. The benefit of the IoE is derived from the combined impact of these connections and the value this increased connectedness creates as 'everything' comes online.

> The next big wave is going to be around the internet of everyting. It will be implemented by combining things with processes, with business changes, with people. And, it will drive a productivity number, and a financial number, that is just mind-boggling.
>
> John Chambers, former CEO, Cisco Systems

1.1.3 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.

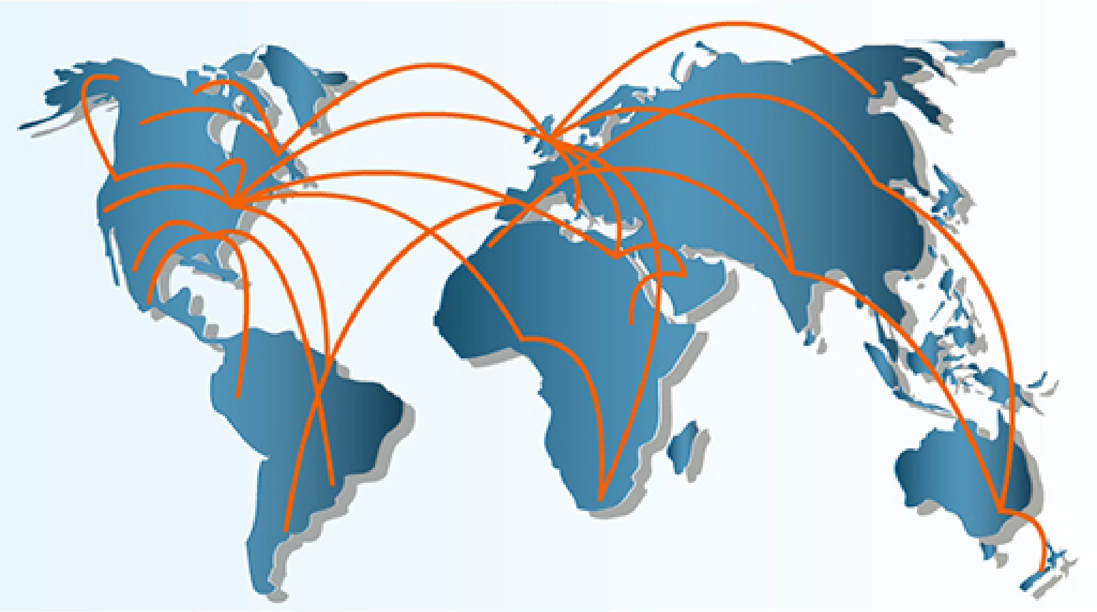


Figure 1 Simplified model of global internet traffic

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.

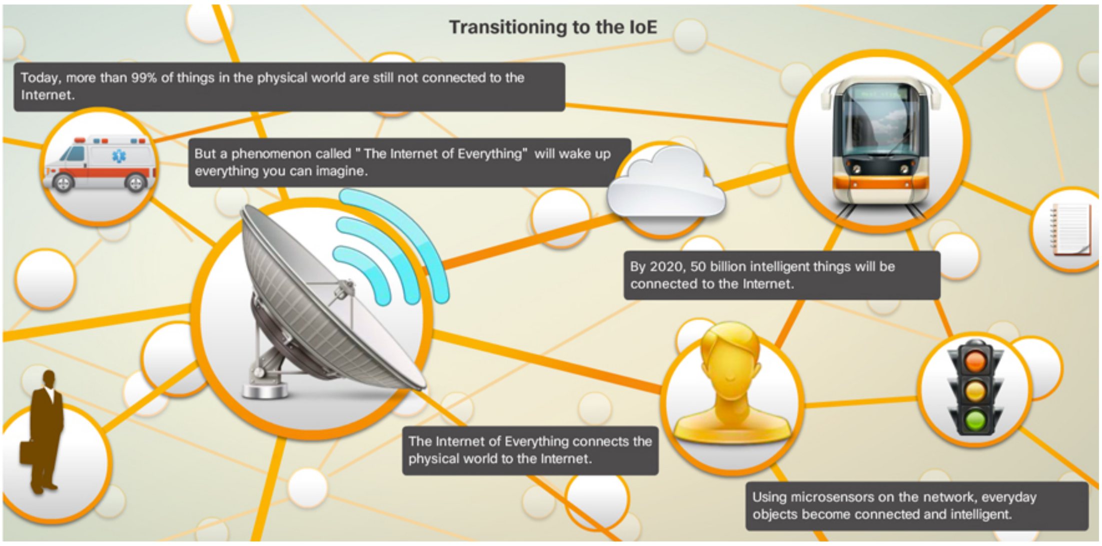
The figure is an oversimplified map of global internet traffic; however, it depicts how countries and continents are connected. View this TeleGgeography map that depicts the location of submarine cables.

After you have opened the 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.

Figure 2 is a connected map that highlights the transition to the IoE. Click on 'view larger image' to see a clearer version.



Transitioning to the IoE

Today, more than 99% of things in the physical world are still not connected to the Internet.

But a phenomenon called " The Internet of Everything" will wake up everything you can imagine.

By 2020, 50 billion intelligent things will be connected to the Internet.

The Internet of Everything connects the physical world to the Internet.

Using microsensors on the network, everyday objects become connected and intelligent.

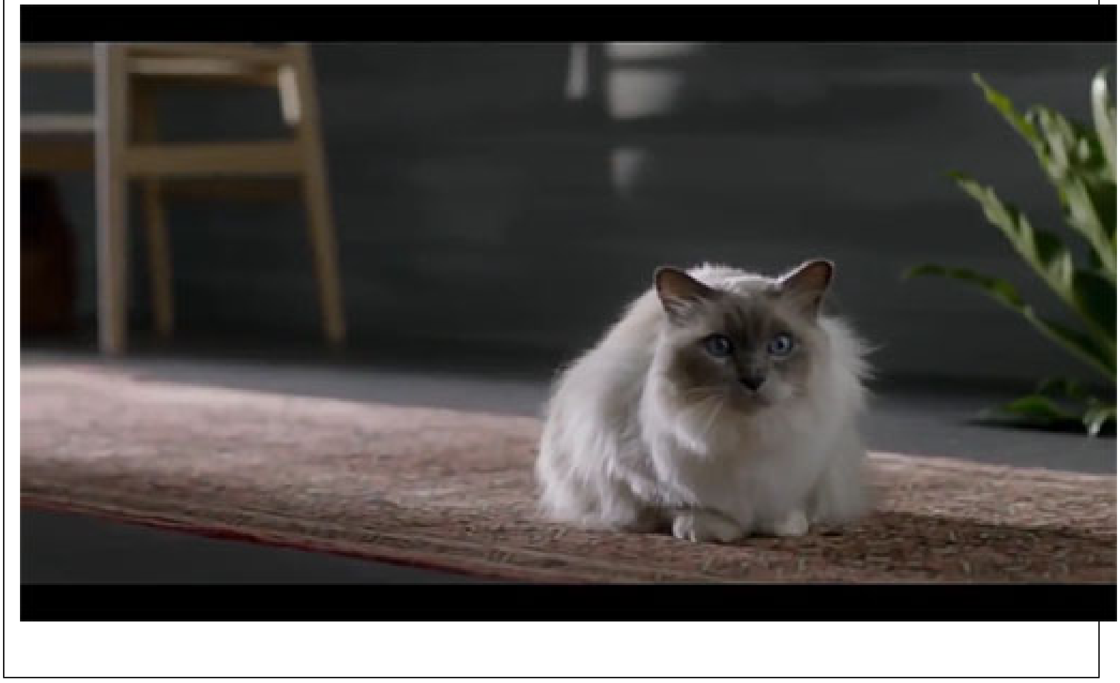
Figure 2 Transitioning to the IoE

1.1.4 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 everything.

Watch Cisco’s vision of how the internet of everything could impact your everyday life.

Video content is not available in this format.



1.1.5 People, process, data and things

The IoE incorporates four pillars to make networked connections more relevant and valuable than ever before: people, process, data, and things. The information from these connections leads to decisions and actions that create new capabilities, richer experiences, and unprecedented economic opportunity for individuals, businesses, and countries.

Table 2 What is the IoE? The internet of Everything is the netowrked connection of people, process, data and things

People	Process	Data	Things
Today, most people connect socially through their web-enabled devices. As the IoE evolves, we will connect in new and valuable ways. Wearable devices and clothing are already changing how we connect.	Processes occur between all of the other pillars in the IoE. With the correct processes, connections become more valuable. These connections provide the right information, delivered to the right person, at the right time and in the most relevant way.	Data is the information generated by people and things. This data, when combined with analytics, delivers actionable information to people and machines. Better decisions are made and better results are achieved.	Things are physical objects that are connected to the internet and to each other. These devices are sensing and collecting more data, becoming context-aware, and providing more experiential information to aid both people and machines.

1.1.6 Interactions of the IoE

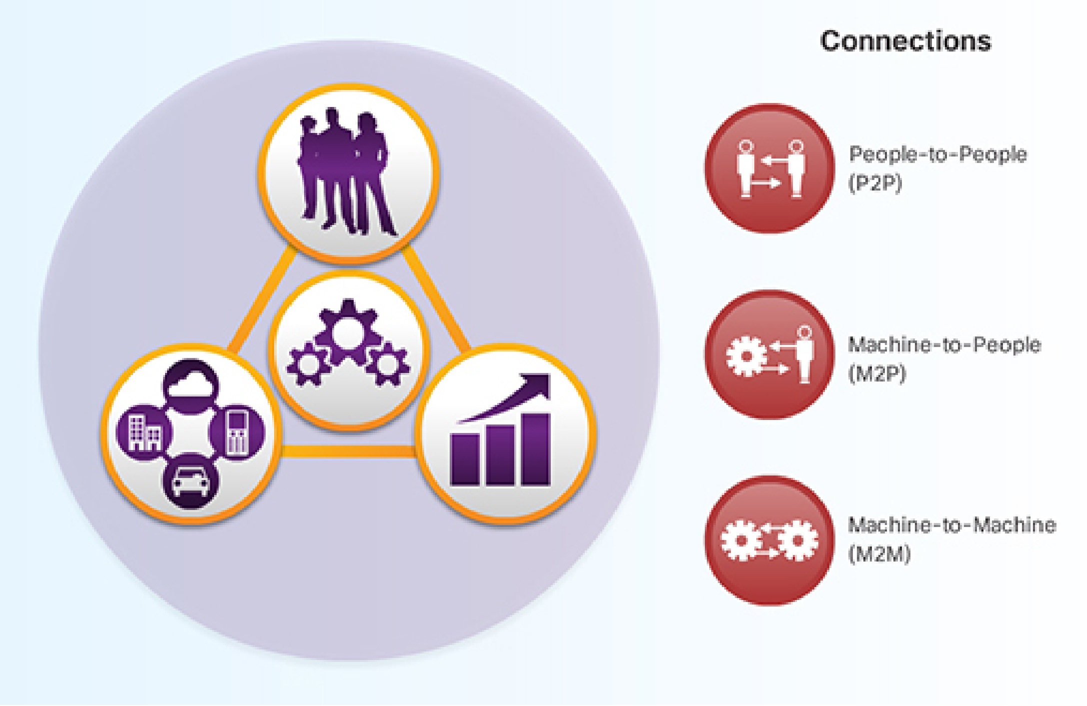


Figure 3 Interactions of the IoE

!Warning! CiscoSansTTLight,Helvetica,Arial,sans-serif not supportedThe interactions between the elements in the four pillars create a wealth of new information. The pillars interact in a way that establishes three main connections in the IoE environment: people communicate with people (P2P), machines communicate with people (M2P), and machines communicate with machines (M2M).

1.2 The value of the IoE

As we become used to the internet of everything, we will need to change the way we behave and use the internet. This isn’t as difficult as it may seem. After all, many of you reading this will have experienced various changes in experience since the popularisation of the internet in the mid 1990s. Many of you have seen the emergence of webmail, online films and music, social media, messaging apps and interactive games (including Pokemon Go). Each relying on the internet and also changing the way that we use it.

1.2.1 Changing behaviours

Figure 4 Heraclitus: Change is the only constant.

People, businesses, and governments must constantly adapt to change.

In 2012, the number of internet-connected devices exceeded the number of people on earth.

With this increased use of technology, people are now exchanging more information, ideas, and opinions than before. The internet is changing the way we communicate, collaborate, and learn. It has changed the way we engage with others and with the products that we use.

People have the ability to react to current news, events, marketing pushes, and products like never before. The ability to gather information and process that information using digital processing power is available at the click of a mouse or the touch of a screen.

1.2.2 Organisations adapt or lose competitive edge

Organisations must be agile and adjust to the changing trends in technology. organisations can use this technology to streamline operational cost through the use of collaboration and automation. In addition, businesses provide more relevant offerings using real-time data gathered from customers.

Organisations must also modify the way they advertise and sell products to customers. Technology is changing individual behaviors, such as how they learn about products, how they compare competitors, and even their purchasing patterns. For this reason, organisations must be able to customise their advertisements and special promotions toward certain customers and cut costs with targeted advertising. Additionally, customers, as a group, can affect the bottom line of the company by expressing their comments online. organisations must be able to react quickly, to counter any negative feedback entered by customers or employees.

These new technologies and trends can lead to tremendous success for some organisations. For other organisations, the failure to adapt to the new trends will likely result in the loss of their competitive edge. They will fail to meet the needs and expectations of the customers they serve. Consider, for example, how internet streaming is affecting the business operations and profit margins of movie rental stores, as shown in the figure. This is also happening with music and printed media.

The IoE forces organisations to adapt, or settle for diminishing impact on their business and society.

Governments and technology

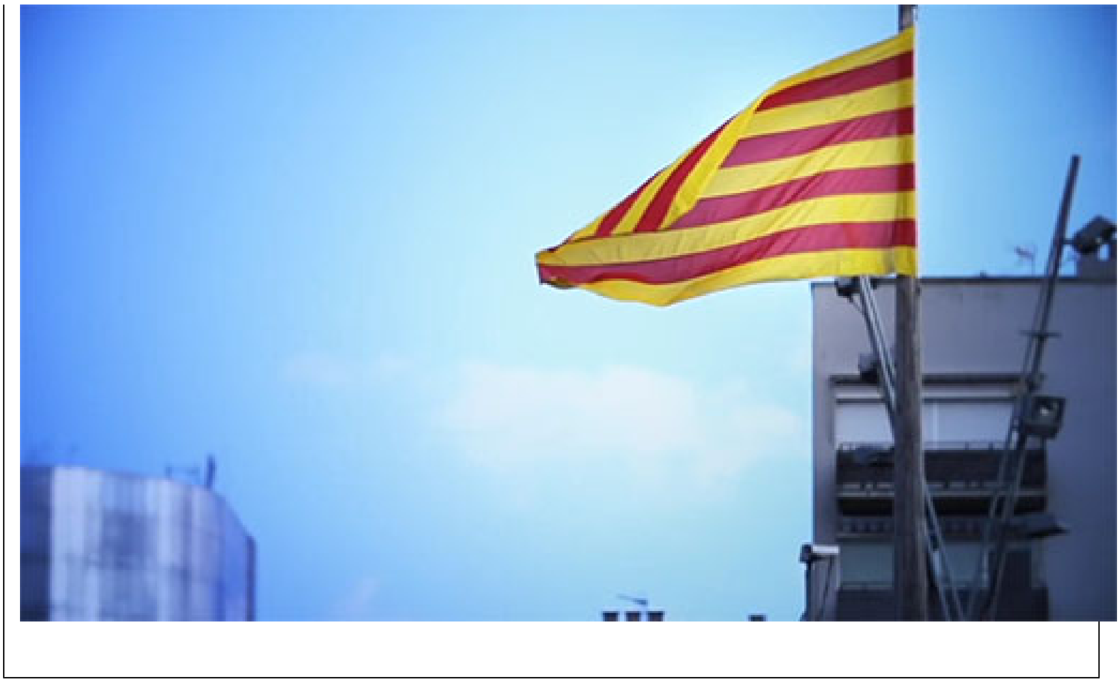
!Warning! CiscoSansTTLight,Helvetica,Arial,sans-serif not supportedGovernments are not immune to the change caused by rapid information exchange through technology. Officials can respond quickly to emergencies through real-time data. Citizens can connect through social media and gather support for change.

1.2.3 Barcelona: a smart city

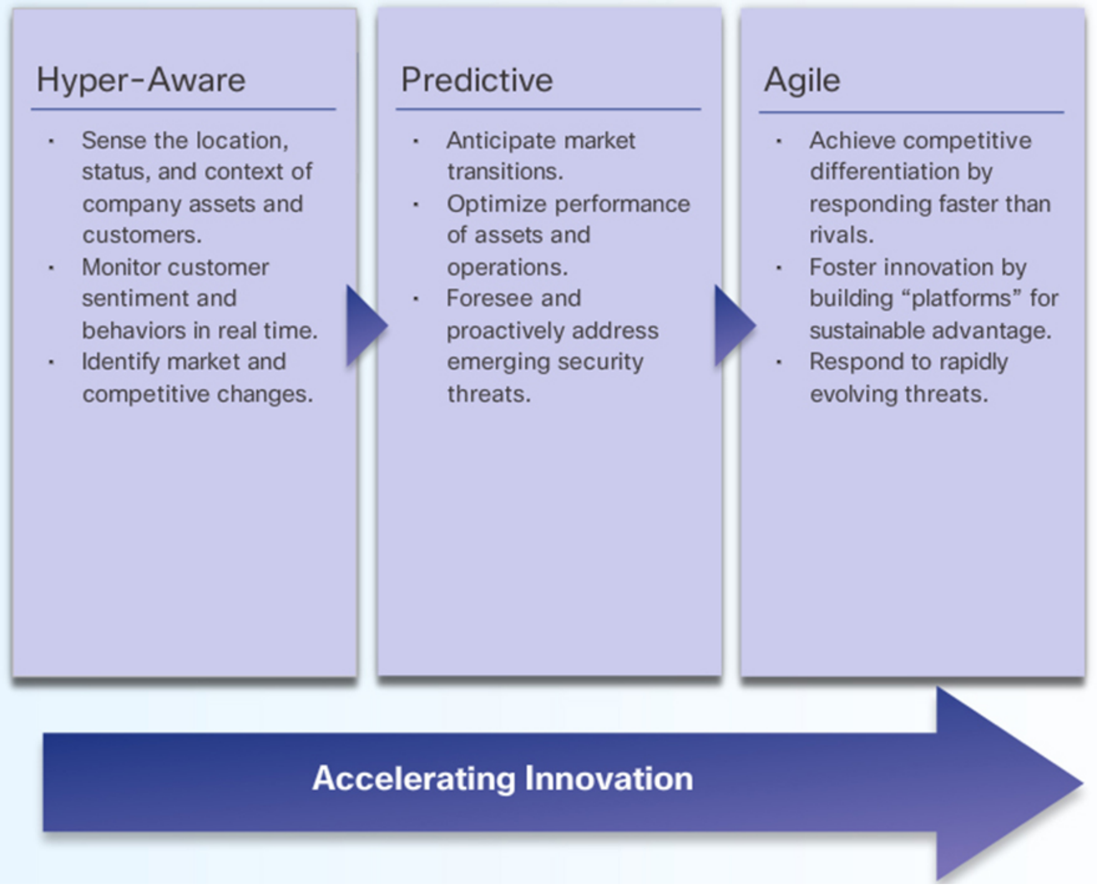
Governments can embrace this technological change, and benefit from it, by incorporating technology into the operation of a city. In 2011, the city council in Barcelona, Spain launched the 'Barcelona as a People City' project. This project uses technical innovations to foster economic growth and the welfare of its citizens.

Watch how Barcelona embraces the IoE to improve the life of its citizens, generate new business opportunities, and reduce operating expenses.

Video content is not available in this format.



1.2.4 Hyper-aware, predictive, agile



Hyper-Aware

- Sense the location, status, and context of company assets and customers.
- Monitor customer sentiment and behaviors in real time.
- Identify market and competitive changes.

Predictive

- Anticipate market transitions.
- Optimize performance of assets and operations.
- Foresee and proactively address emerging security threats.

Agile

- Achieve competitive differentiation by responding faster than rivals.
- Foster innovation by building “platforms” for sustainable advantage.
- Respond to rapidly evolving threats.

Figure 5 Hyper-aware, predictive, agile

What does it mean to be IoE-ready? IoE-ready is characterised by three critical attributes:

- hyper-awareness – sensors can capture real-time data on products
- ability to predict – new types of data analysis tools allow an organisation to forecast future trends and behaviours
- agility – increasingly accurate predictions allow organisations to be more responsive and flexible to emerging marketplace trends and threats.

Combining these three attributes allows organisations to better create, communicate, and deliver their offerings.

1.2.5 IoE and industries

For organisations to realise the potential value of the IoE, they must focus on the IoE-driven capabilities that most benefit their organisation. This can vary across industries.

Table 3 displays some of the potential uses of the IoE across multiple industries, including manufacturing, energy firms, and retail organisations.

Table 3 The use of the IoE in industries

Manufacturing	Energy firms	Retail
IoE capabilities may include real-time, multidimensional data analysis, intergrated video collaboration, and remote tracking of physical assets.	IoE capabilities may include integration of sensor data, ability to direct staff, and predictive analytics.	IoE capabilities may include video, customer behaviour analysis, data analytics and visualisation, and location-based marketing on any device.

The IoE affects five core priorities of an organisation (Table 4).

Table 4 Core priorities

Customer experience	Innovation	Employee productivity	Asset utilisation	Supply
Improving customer relationships to garner more of the market.	Reducing time to market products and improving product development to meet customer needs.	Providing the ability to be more productive and scalable.	Lowering costs.	Identifying areas of waste and delay, while increasing logistical efficiency.

1.2.6 Maximising IoE value

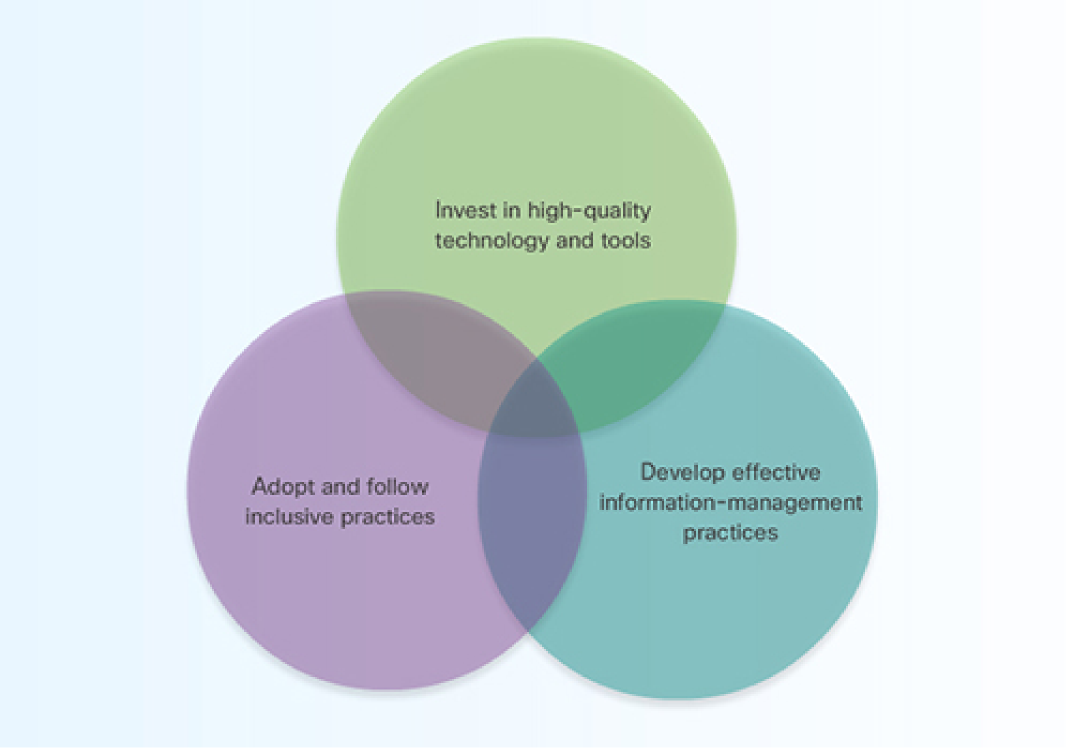

Invest in high-quality technology and tools
Adopt and follow inclusive practices
Develop effective information-management practices

Figure 6 Venn diagram demonstrating the value-link between tools,management and practices

For organisations to join the IoE economy, and maximise the value of their IoE implementation, organisations must consider:

- **Investing in a high-quality technology infrastructure and tools** – A secure and reliable network infrastructure is required to support the IoE.
- **Adopting and following inclusive practices** – An inclusive environment is one in which the employees of that environment feel as though they are part of the change. It is an open atmosphere where individuals feel that they are included.
- **Developing effective information-management practices** – Management must be able to embrace and promote change. Information sharing and management must be supported, and data extracting techniques must be developed so that the right information is provided at the right time, to the right people and things.

Organisations are able to achieve a significant competitive advantage by adapting their business processes through the use of IoE technologies.

1.2.7 Internet of everything and Cisco

Cisco is uniquely positioned in that it has end-to-end solutions already within its product line, and is continuing to innovate to support the IoE. Cisco’s contribution to the IoE is the software, hardware, and platforms that support the internet. These platforms will enable the next phase of the IoE.

Watch Dave Evans, Cisco's Chief Futurist, describing how the IoE will change the world for the better by creating more relevant and valuable connections.

Video content is not available in this format.

Learn more about the IoE at Cisco’s IoE website.

1.3 Globally connected

The reality is that we are all globally connected. For many of us, our friends on social media no longer reside down our street or in our town. Humanity has become globally connected and the internet has offered us a way to stay in touch professionally and personally with like minded souls.

Networking technology provides this foundation, the internet is after all a network of interconnected networks. From your home network to large corporate systems the shape of the internet is continually changing and offering us new ways to interconnect technologies such as the IoE.

1.3.1 Networks are the foundation

!Warning! CiscoSansTTLight,Helvetica,Arial,sans-serif not supportedFifty billion things provide trillions of gigabytes of data. How can they work together to enhance our decision-making and interactions to improve our lives and our businesses? Enabling these connections are the networks that we use daily. These networks provide the foundation for the internet and, ultimately, the IoE.

Networks continue to evolve

!Warning! CiscoSansTTLight,Helvetica,Arial,sans-serif not supportedThe methods that we use to communicate continue to evolve. Whereas we were once limited to face-to-face interactions, breakthroughs in technology have significantly extended the reach of our communications. From cave paintings, to the printing press, to radio, to television, and to telepresence, each new development has enhanced our ability to communicate with others.

Networks of many sizes

Networks form the foundation of the IoE. 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 sharing of resources, such as printers, documents, pictures, and music between a few local computers.

In businesses and large organisations, 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. In fact, the term internet means a 'network of networks'. The internet is literally a collection of interconnected private and public networks. Businesses, small office networks, and even home networks usually provide a shared connection to the internet.

Table 5 Four types of network

Small home networks	Small office/home office networks	Medium to large networks	World wide networks
Small home networks connect a few computers to each other and the internet.	The small office/home office network enables computers to connect to a corporate network, to access resources.	Medium to large networks can have many locations with thousands of interconnected computers. These networks could include newer places in the network (PINs). Examples are plant area networks (PANs) and field area networks (FANs) that extend the reach and power of the network for new applications and devices.	The internet is a network of networks that connects hundreds of millions of computers everywhere.

1.3.2 Components of the 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.

Click each button in the figure to highlight the corresponding network components.

Interactive content is not available in this format.

Figure 7 Network components

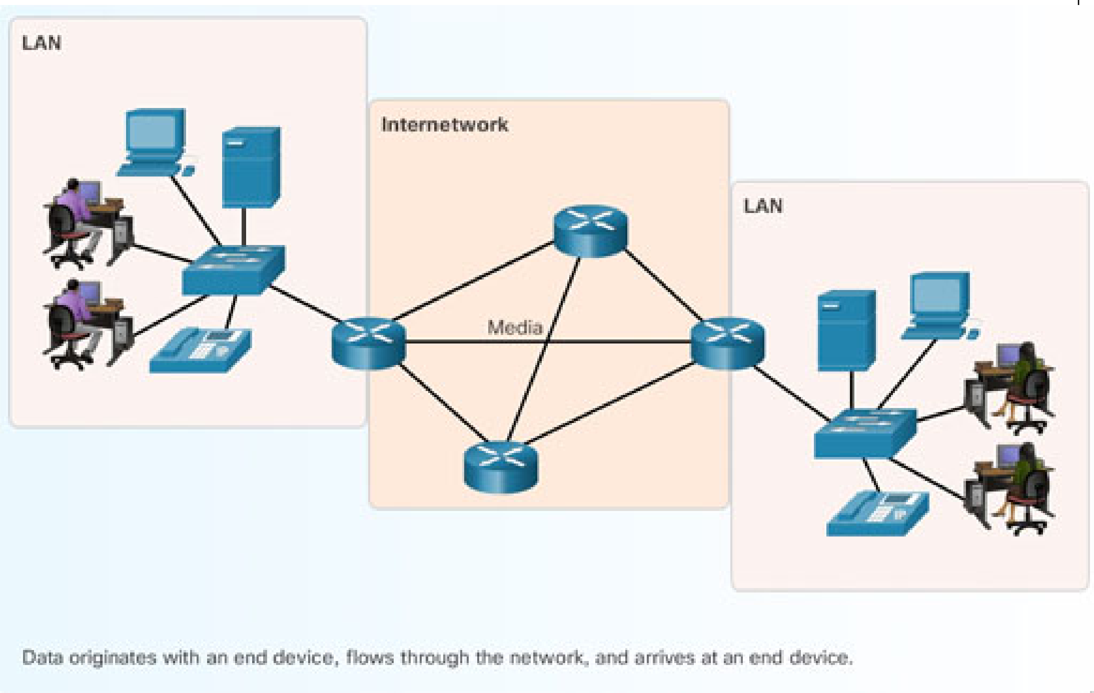
Devices and media are the physical elements, or hardware, of the network. Hardware is often the visible components of the network platform such as a laptop, PC, switch, router, wireless access point, or the cabling used to connect the devices. Occasionally, some components may not be so visible. In the case of wireless media, messages are transmitted through the air using invisible radio frequency or infrared waves.

Network components are used to provide services and processes. These are the communication programs, called software, that run on the networked devices. A network service provides information in response to a request. Services include many of the common network applications people use every day, like email hosting services and web hosting services. Processes provide the functionality that directs and moves the messages through the network. Processes are less obvious to us but are critical to the operation of networks.

1.3.3 End devices

The following animation shows an IP packet being sent from one end device to another. Click on the full screen button to view.

Video content is not available in this format.


LAN
Internetwork
Media
LAN
Data originates with an end device, flows through the network, and arrives at an end device.

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)
- nsetwork printers
- VoIP phones
- TelePresence endpoints
- security cameras
- mobile handheld devices (smartphones, tablets, PDAs, and wireless debit/credit card readers and barcode scanners)sensors such as thermometers, weight scales, and other devices that will be connected to the 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. Figure 8 provides a brief description of each. Press each plus symbol to view the end device to server interaction.

Interactive content is not available in this format.

Figure 8 End devices

1.3.4 Intermediary network devices

Video content is not available in this format.

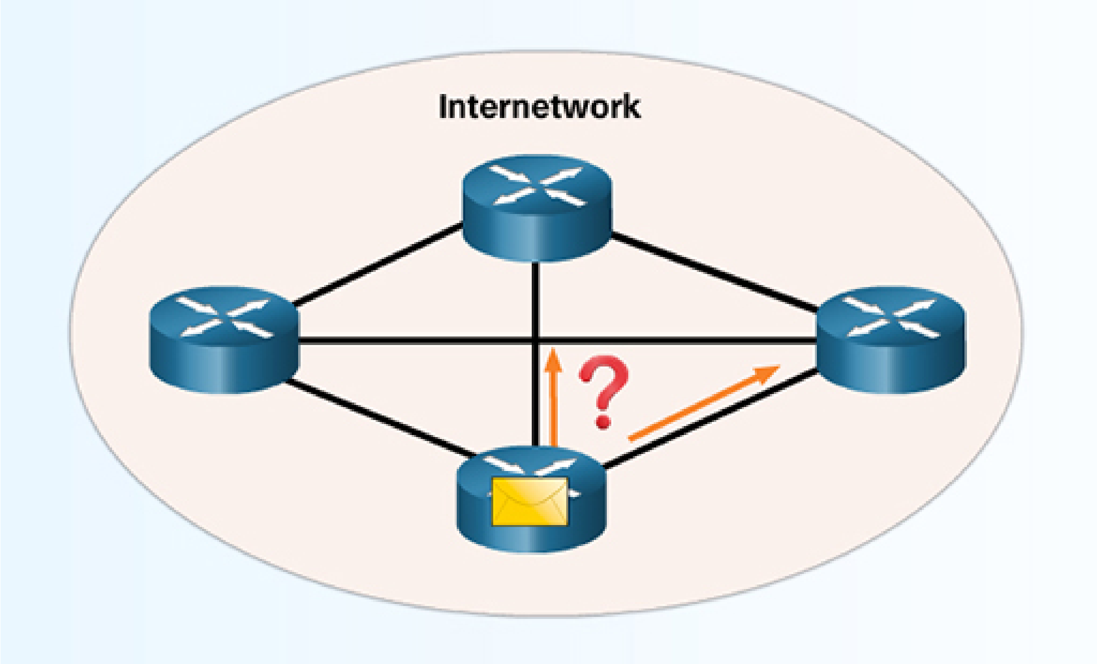


Figure 9 Intermediary devices determine the path of the data, but do not generate or change the data content.

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

Examples of intermediary network devices 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 intermediary 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 intermediary 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 ofsService (QoS) priorities
- permit or deny the flow of data, based on security settings.

1.3.5 Network media

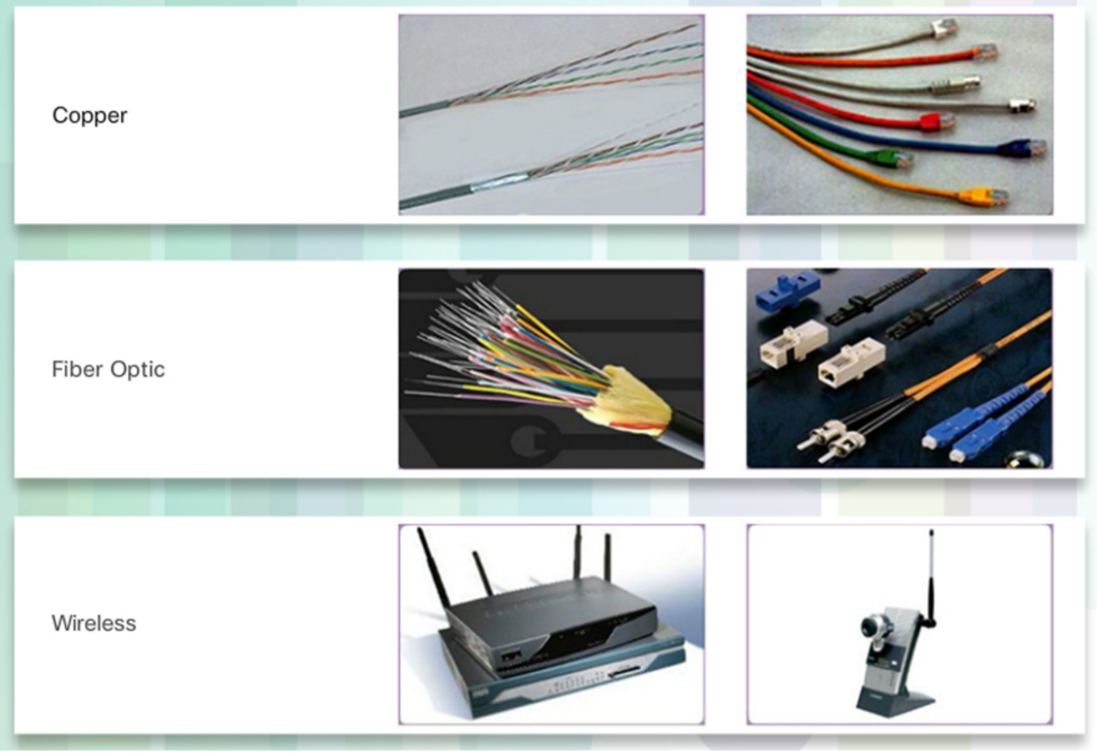


Figure 10 Types of network connection media

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 fibres (fibre 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.

1.3.6 Types of networks

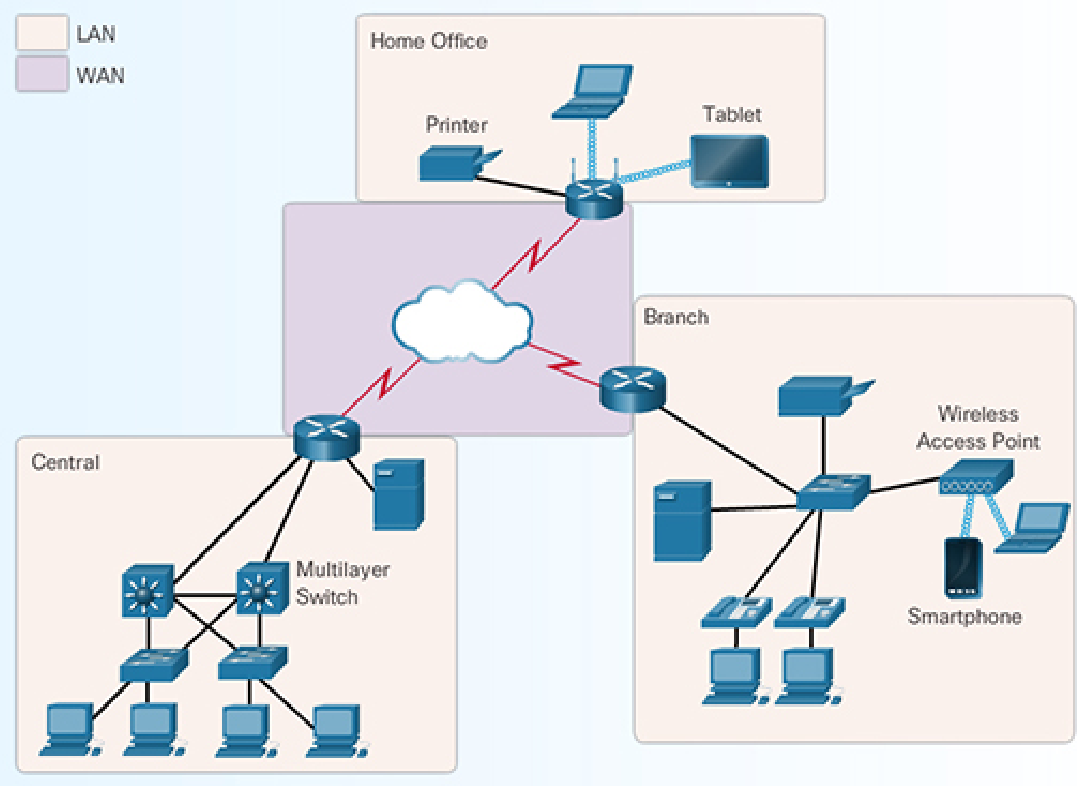


Figure 11 Types of network connection media

Network infrastructures can vary greatly in terms of:

- size of the area covered
- number of users connected
- number and types of services available.

Figure 11 illustrates the two most common types of network infrastructure:

- **Local area network (LAN)** −a network infrastructure that provides access to users and end devices in a limited area such as a home, school, office building, or campus. It provides high speed bandwidth to internal end devices and intermediary devices.

- **Wide area network (WAN)** − a network infrastructure that interconnects LANs over wide geographical areas such as between cities, states, provinces, countries, or continents. WANs are usually owned by an autonomous organisation, such as a corporation or a government. WANs typically provide link speeds between LANs that are slower than the link speeds within a LAN.

1.3.7 The internet is bringing the world together

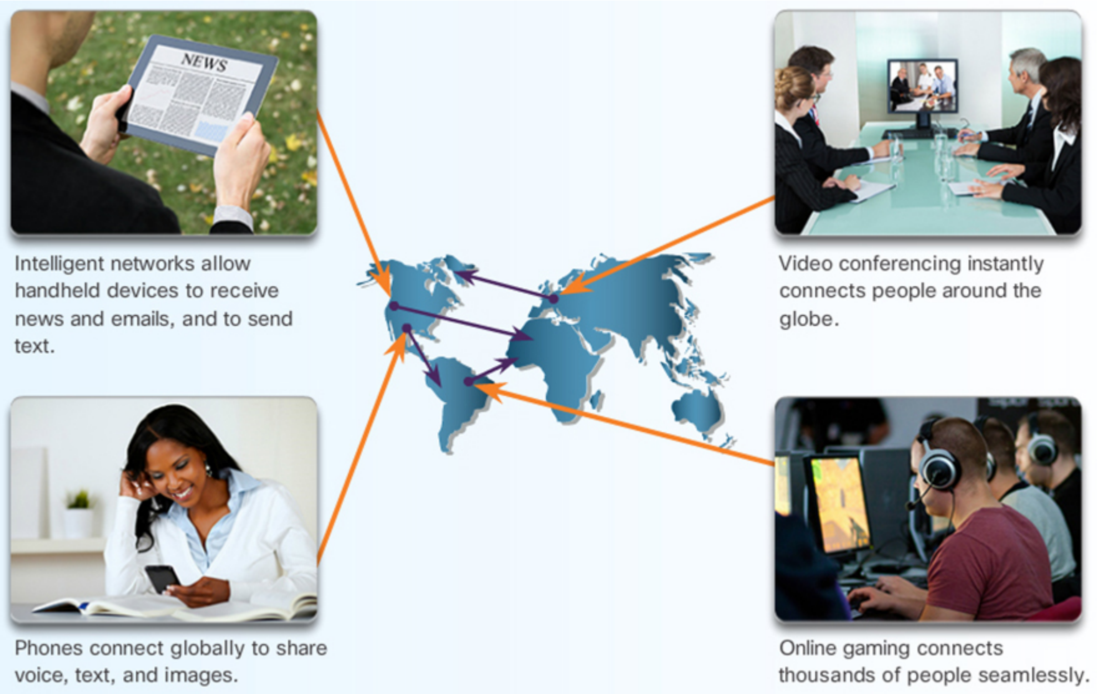

Intelligent networks allow handheld devices to receive news and emails, and to send text.
Video conferencing instantly connects people around the globe.
Phones connect globally to share voice, text, and images.
Online gaming connects thousands of people seamlessly.

Figure 12 Intelligent networks

Although there are benefits to using a LAN or WAN, most individuals need to communicate with a resource on another network. This network may be outside of the local network. This communication is achieved using the internet.

The internet is not owned by any individual or group. The internet is a worldwide collection of interconnected networks (internetworks or internet for short), cooperating with each other to exchange information using common standards. Through telephone wires, fibre optic cables, wireless transmissions, and satellite links, internet users can exchange information in a variety of forms, as shown in the figure.

1.3.8 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.

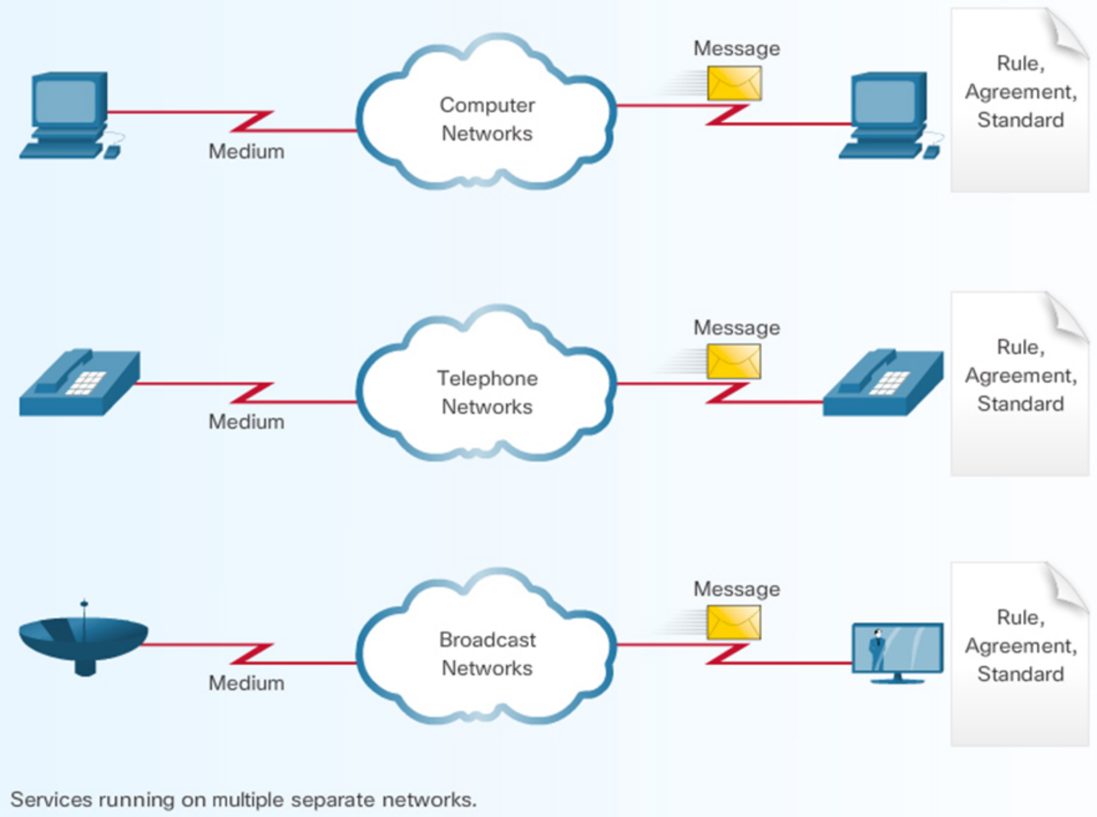

Message
Computer Networks
Medium
Rule, Agreement, Standard
Message
Telephone Networks
Medium
Rule, Agreement, Standard
Message
Broadcast Networks
Medium
Rule, Agreement, Standard
Services running on multiple separate networks.

Figure 13 Services running on multiple separate networks

Consider some schools that were cabled for a computer network 30 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 13.

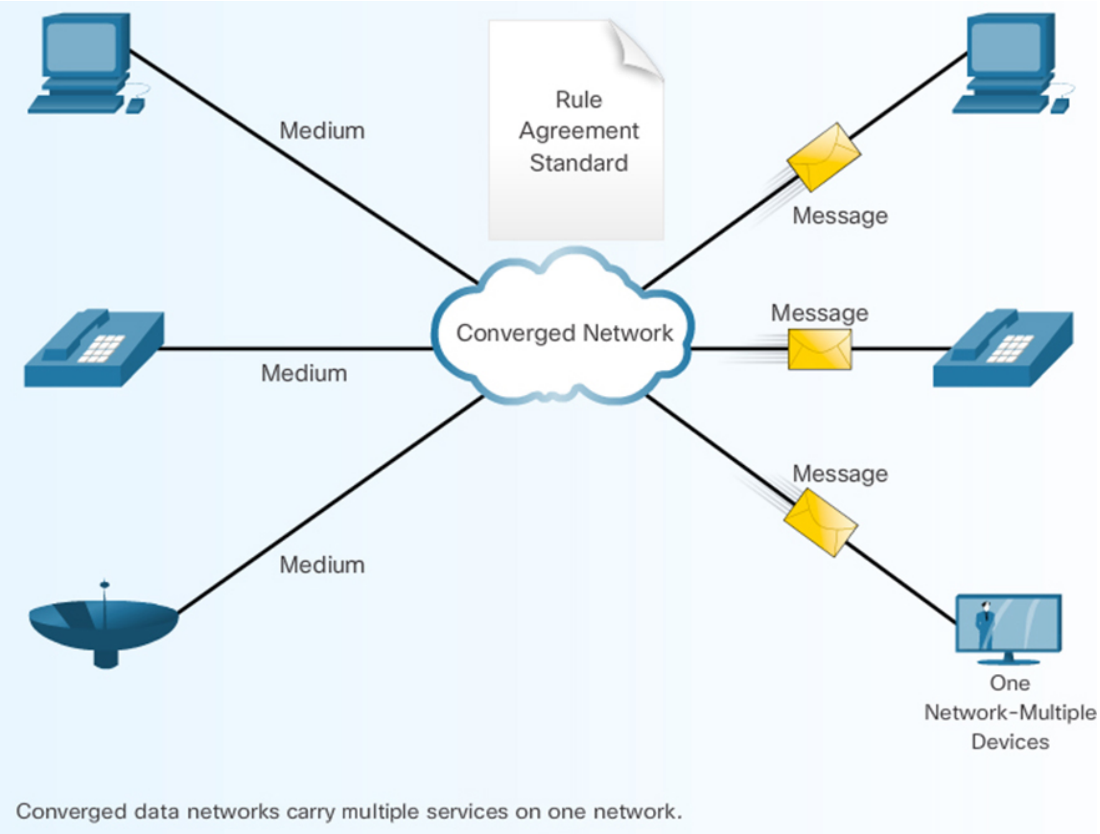
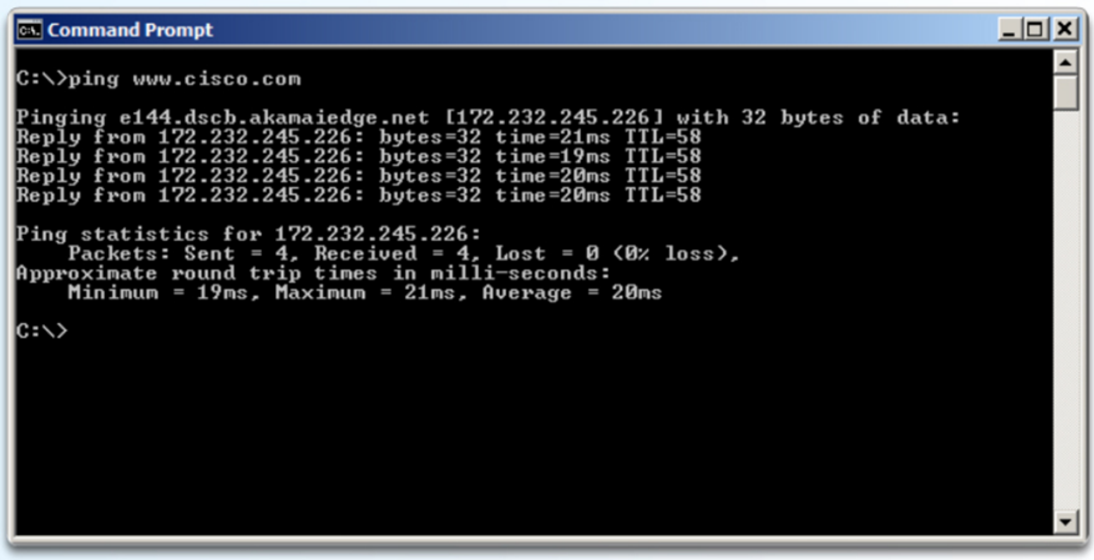


Figure 14 Converged data networks carry multiple services on one network.

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 streams, text, and graphics between many different types of devices over the same communication channel and network structure, as shown in Figure 14. 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 specialised 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.

1.3.9 Lab: mapping the internet



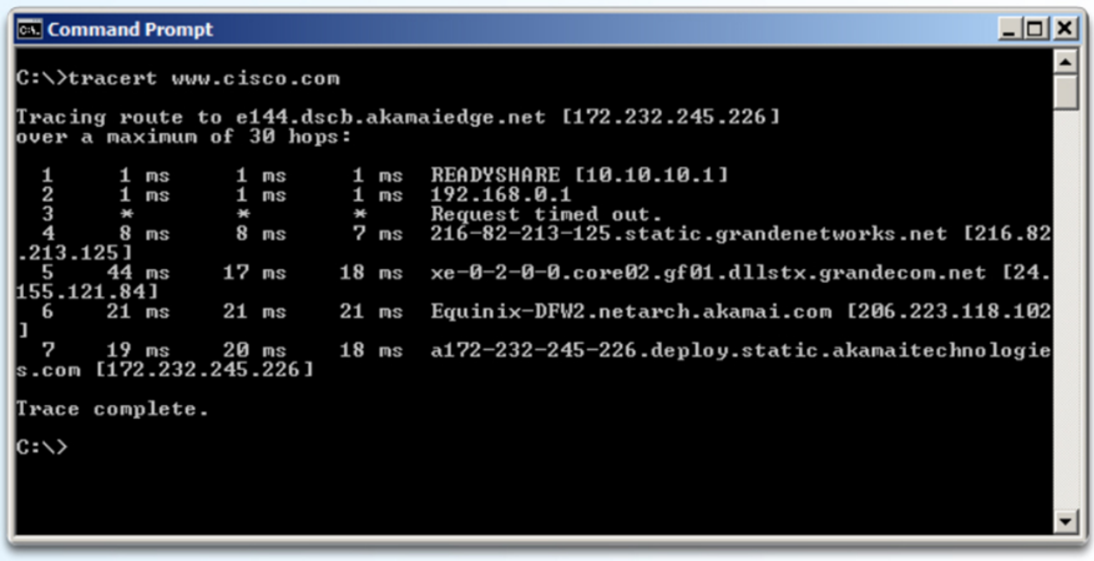
```
C:\>ping www.cisco.com

Pinging e144.dscb.akamaiedge.net [172.232.245.226] with 32 bytes of data:
Reply from 172.232.245.226: bytes=32 time=21ms TTL=58
Reply from 172.232.245.226: bytes=32 time=19ms TTL=58
Reply from 172.232.245.226: bytes=32 time=20ms TTL=58
Reply from 172.232.245.226: bytes=32 time=20ms TTL=58

Ping statistics for 172.232.245.226:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 19ms, Maximum = 21ms, Average = 20ms

C:\>
```

Figure 15 Ping output



```
C:\>tracert www.cisco.com

Tracing route to e144.dscb.akamaiedge.net [172.232.245.226]
over a maximum of 30 hops:

  1     1 ms     1 ms     1 ms  READYSHARE [10.10.10.1]
  2     1 ms     1 ms     1 ms  192.168.0.1
  3     *        *        *     Request timed out.
  4     8 ms     8 ms     7 ms  216-82-213-125.static.grandenetworks.net [216.82
.213.125]
  5    44 ms    17 ms    18 ms  xe-0-2-0-0.core02.gf01.dllstx.grandecom.net [24.
155.121.84]
  6    21 ms    21 ms    21 ms  Equinix-DFW2.netarch.akamai.com [206.223.118.102
]
  7    19 ms    20 ms    18 ms  a172-232-245-226.deploy.static.akamaitechnologie
s.com [172.232.245.226]

Trace complete.

C:\>
```

Figure 16 Tracert output

Would you like to see how long it takes for data to travel from your computer to a remote destination and back? In Figure 15, the ping command took an average of 20 milliseconds to receive a reply from the server at www.cisco.com.

Would you like to see the path that data travels to reach a destination? In Figure 16, the **tracert** command generated a path showing that data passed through seven intermediary devices on its way from source to destination.

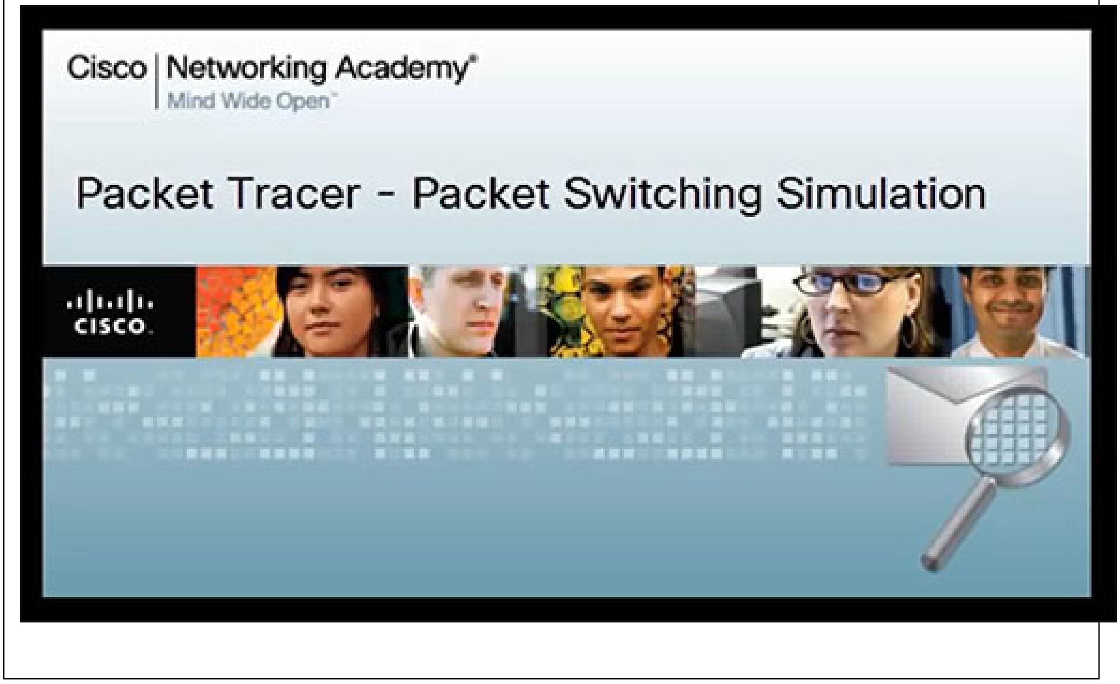
Network administrators and technicians use **ping** and **tracert** to test network connectivity and resolve problems. To further explore these two utilities, download Lab - Mapping the internet.

1.3.10 Packet tracer: packet switching simulation

Packet Tracer is a fun, take-home, flexible software program that allows you to experiment with network behavior, build network models, and ask 'what if' questions. In this activity, you will explore how Packet Tracer serves as a modeling tool for network representations. While doing so, you will explore a simulation of how packets are created and sent across the network traveling from source device to destination device.

Watch this demonstration of the Packet Tracer – Packet Switching Simulation activity.

Video content is not available in this format.


Cisco | Networking Academy®
Mind Wide Open™
Packet Tracer - Packet Switching Simulation
cisco

The video demonstration is the primary source for how to navigate the activity. However, after viewing the video, you can download the following files to investigate the activity on your own.

- Packet Tracer – Packet Switching Simulation.pdf
- Packet Tracer – Packet Switching Simulation A.pkz
- Packet Tracer – Packet Switching Simulation B.pkz

Essential note: If you are new to Packet Tracer, you can watch a tutorial. You must install Packet Tracer before you can open .pkz files. To install Packet Tracer, return to the course progress page where a copy is available to download and install .

Packet Tracer is available for both Microsoft Windows and Linux systems. The Open University Cisco Academy team support a moderated Facebook Community helping Mac users port this application onto all versions of the Apple Mac OSX. For more information, you will need to join the community.

Cisco also offer a free course on how to use Packet Tracer and how to obtain a free copy.

1.3.11 Planning for the future

The convergence of the different types of networks onto one platform represents the first phase in building the intelligent information network that will support the IoE. This convergence includes consolidating the applications that generate, transmit, and secure data. The underlying processes that drive this explosive growth have resulted in a network architecture that is both capable of supporting change and expansion. It is this converged network that serves as the fundamental building block for the IoE.

Watch the video of real-life experiences of business owners, government officials, and healthcare providers as they work towards making the IoE a reality.

Video content is not available in this format.

1.4 Terms and concepts practice

This activity will help you to test some of the terms and concepts you've been introduced to.

converged networks

LAN

WAN

end device

intermediary

people

things

data

M2M

M2P

P2P

Match each of the items above to an item below.

data, voice, and video all use the same network media

provides access to users and end devices in a limited area

interconnects LANs over a broad geographic area

the source and destination of messages transmitted over a network

device connects individual hosts to the network or connects networks to each other

exchange information, ideas, and opinions through the use of data and technology

physical objects with sensors that are connected to a network

collected and transmitted by people and connected things

machine to machine

machine to people

people to people

1.5 Session 1 quiz

Check what you have learned in Session 1.

Session 1 quiz.

Use 'ctrl' (cmd on a Mac) or right-click to open the quiz in a new window or tab then come back here when you're finished.

1.6 Summary

The evolution of the internet has witnessed four distinct phases:

- connectivity
- networked economy
- collaborative experience
- the internet of everything (IoE).

The internet is essentially a network of networks. Underneath this network of networks lies a very real backbone of connections that bring the world to our internet-enabled devices. The IoE is bringing together:

- people
- process
- data
- things.

There are three main connections in the IoE environment:

- people communicate with people (P2P)
- machines communicate with people (M2P)
- machines communicate with machines (M2M).

The IoE brings value to organisations in these five areas:

- customer experience
- innovation
- employee productivity
- asset utilisation
- supply.

Networks provide the foundation for the internet and, ultimately, the IoE. The components of a network fall into one of three categories:

- devices
- media
- services.

The two most common types of networks are LAN and WAN. Consolidating different types of networks onto one platform creates a 'converged network'. Unlike dedicated networks, converged networks are capable of delivering voice, video streams, text, and graphics between many different types of devices over the same communication channel and network structure.

Session 2: Pillars of the IoE

2.1 The four pillars

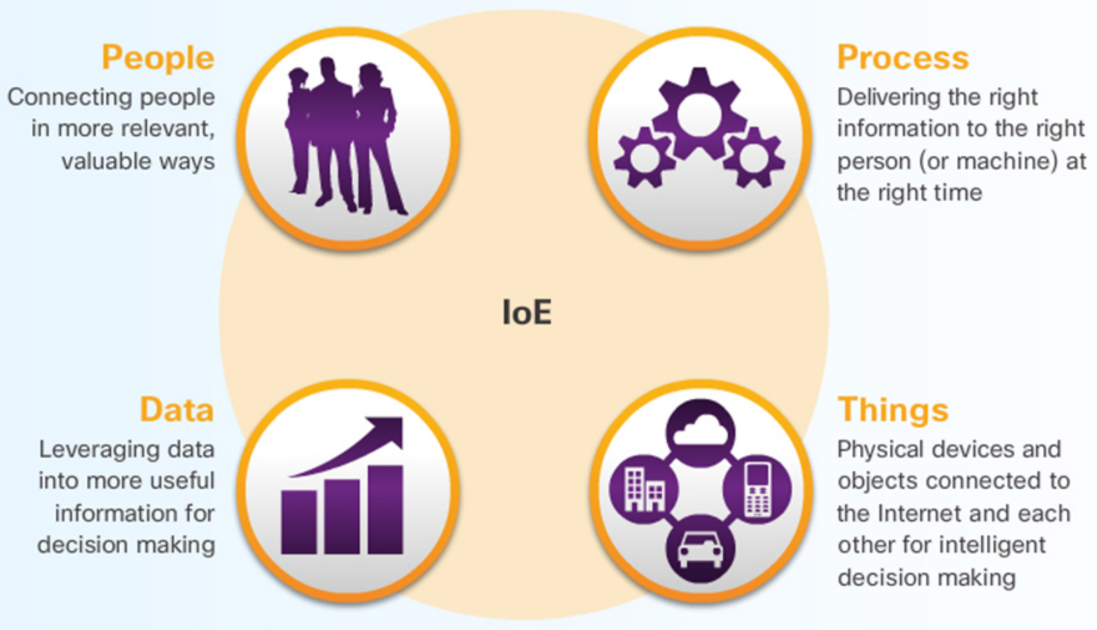

People
Connecting people in more relevant, valuable ways
Process
Delivering the right information to the right person (or machine) at the right time
IoE
Data
Leveraging data into more useful information for decision making
Things
Physical devices and objects connected to the Internet and each other for intelligent decision making

Figure 1 The four pillars

The idea of connecting things is not a new one. In fact, the internet of things (IoT) is a term that has been broadly accepted since the late 1990s. The IoT refers to the network of physical objects accessible through the internet.

Not all of the objects that connect to the IoT will be computing devices, but many will be. So, what is a computing device? While it may be easy to identify a desktop or a laptop computer, the line between what is and is not a computer can become blurred. Is a car a computing device? What about a watch or a television?

The first computing devices (computers) were huge, room-sized machines that took teams of people to build, manage and maintain. Today, they are exponentially faster and only a fraction of the size of their predecessors. For the purposes of this course, a computing device is an electronic machine that performs calculations based on a set of instructions and comprises three main components: a central processing unit (CPU), memory, and an input/output unit.

Based on the definition above, a digital watch is a computing device, but an analogue watch is not. The digital watch has a CPU to run its program, it has memory to store the program and other information, and it has an I/O device to allow user interaction (screen, display, buttons, sound alerts, etc.). Although the analogue watch has the I/O component, it lacks CPU and memory.

2.1.1 What are things?

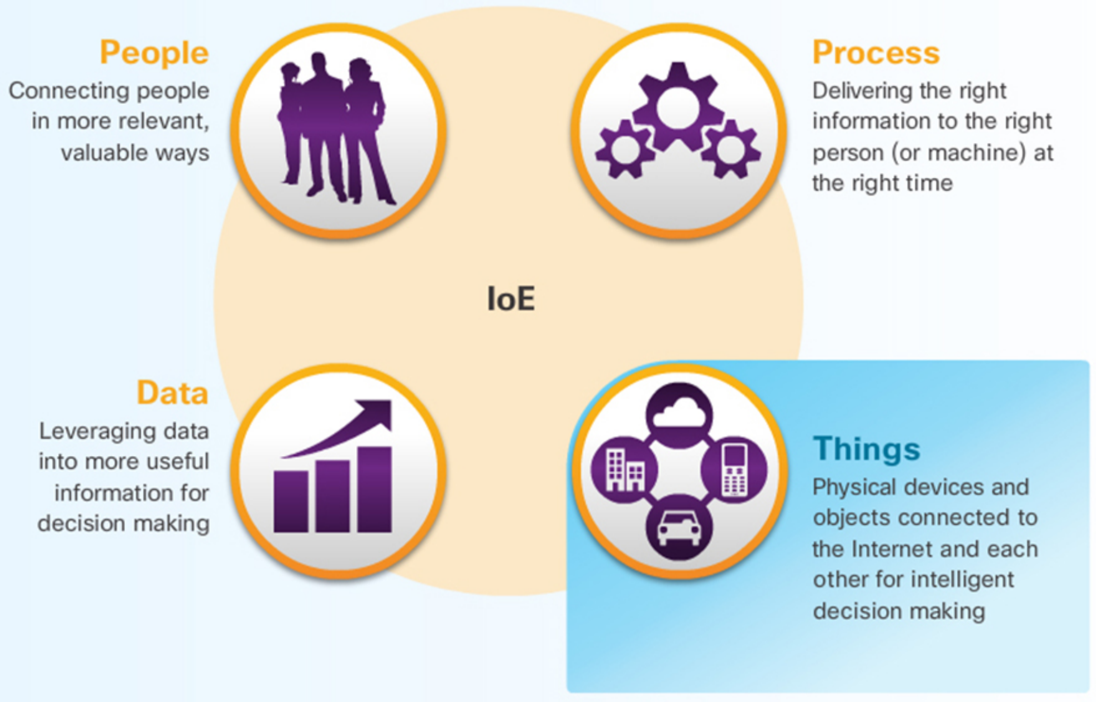

People
Connecting people in more relevant, valuable ways
Process
Delivering the right information to the right person (or machine) at the right time
IoE
Data
Leveraging data into more useful information for decision making
Things
Physical devices and objects connected to the Internet and each other for intelligent decision making

Figure 2 The four pillars: things

Currently, the things pillar, highlighted in Figure 2, comprises various types of traditional computers and computing devices, such as desktops, laptops, smartphones, tablets, mainframes, and computer clusters. However, the IoT will include all types of objects, including objects and devices that are not traditionally connected. In fact, Cisco estimates that 99 percent of physical objects will one day be connected.

These objects contain embedded technology to interact with internal servers and the external environment. These objects are network-capable, and can communicate across a secure, reliable and available network platform. However, the IoT refers to a single technology transition; the ability to connect objects that were previously unconnected so those objects can communicate across the network.

The availability of data, when objects can sense and communicate, has the capability of changing how and where decisions are made, who makes the decisions, and the processes that individuals and businesses use to make those decisions. The IoE is built on the connections among people, processes, data, and things. These are the four pillars of the IoE, as shown in the figure. However, the IoE is not about these four dimensions in isolation. Each amplifies the capabilities of the other three. It is in the intersection of all of these elements that the true power of the IoE is realised.

2.1.2 Common devices

The internet connects more computing devices than just desktop and laptop computers. There are devices all around that you may interact with on a daily basis that are also connected to the internet.

For example, people are using mobile devices more every day to communicate and accomplish daily tasks, such as checking the weather or online banking. The table below shows more about mobile devices.

In the future, many of the things in your home could also connect to the internet so that they can be monitored and configured remotely. Table 1 shows more about connected household devices.

There are also many connected devices found in the world outside your home that provide convenience and useful or even vital information. The table below shows more about these commonly found connected devices.

How many of these devices do you use on a daily basis?

Table 1 Common types of devices

Smartphones	Tablets	Smartwatches	Google Glass
Smartphones are able to connect to the internet from almost anywhere. Smartphones combine the functions of many different products together, such as a telephone, camera, GPS receiver, media player, and touch screen computer.	Tablets, like smartphones, also have the functionality of multiple devices. With the additional screen size, they are ideal for watching videos and reading magazines or books. With on-screen keyboards, users are able to do many of the things they used to do on their laptop computer, such as composing emails or browsing the web.	A smartwatch can connect to a smartphone to provide the user with alerts and messages. Additional functions, such as heart rate monitoring and counting steps, like a pedometer, can help people who are wearing the device to track their health.	Google glass was an experimental wearable computer in the form of glasses with a tiny screen that displays information to the wearer in a similar fashion to the head-up display (HUD) of a fighter pilot. A small touch pad on the side allows the user to navigate menus while still being able to see through the Google glass.

2.1.3 Connecting devices

For the IoE to function, all of the devices that are part of the intended IoE solution must be connected together so that they can communicate. There are two ways to connect devices: wired or wirelessly.

In most cases, connecting devices together using cables is too costly or cumbersome to be practical. For this reason, most devices will need to send and receive data wirelessly.

There are many different types of wireless communication. The most common types of wireless communication are Wi-Fi, Cellular, Bluetooth, and near field communication (NFC). Some devices, such as smartphones and tablets use a combination of wireless communication methods to connect to different devices.

Figure 3 details how a smartphone may connect to other types of devices. Click on each of the plus signs to interact with the image.

Interactive content is not available in this format.

Figure 3 Smartphone connections

2.1.4 Electronics that are not on the internet

According to Internet World Stats, as of June 2012, statistical data indicates that there were approximately 2.4 billion users on the Internet. This is only 34% of the total world population.

The number of connected devices on the internet in 2012 exceeded the world population. This includes traditional computing devices and mobile devices, as well as new industrial and consumer devices that we think of as 'things'.

Although, this may seem like a lot of devices on the internet, it represents less than 1% of the objects that could be connected. Some examples of devices that are currently unconnected could include microwaves, alarm clocks, and lighting systems.

2.1.5 Sensors

Sensors are one way to collect data from non-computers. They convert physical aspects of our environment into electrical signals that can be processed by computers. Some examples are soil moisture sensors, air temperature sensors, radiation sensors, and motion sensors. Sensors of all types will play an important role in connecting what has traditionally been unconnected in the IoE.

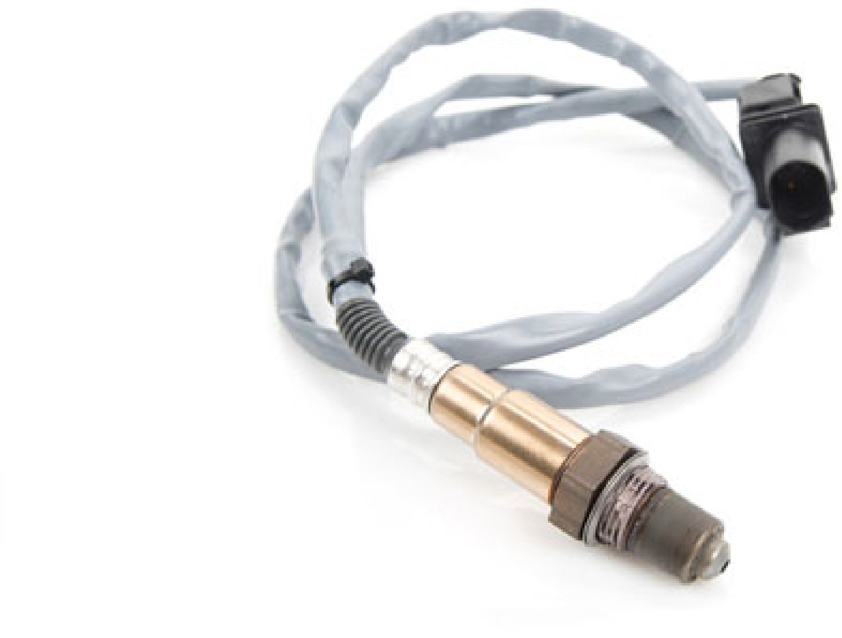


Figure 4 Car oxygen sensor

Figure 4 shows an oxygen sensor. These sensors are very common in cars equipped with electronic fuel injection and are used to monitor the amount of oxygen expelled by the engine after a cycle of fuel burn. Based on that information, the fuel injection computer is able to adjust the air-fuel mixture for optimal engine performance

2.1.6 RFID

A popular type of sensor uses radio frequency identification (RFID). RFID uses radio frequency electromagnetic fields to communicate information between small coded tags (RFID tags) and an RFID reader. Usually, RFID tags are used to identify and track what they are embedded into, such as a pet. Because the tags are small, they can be attached to virtually anything including clothing and cash. Some RFID tags carry no batteries. The energy required by the tag to transmit information is obtained from the electromagnetic signals that are sent by the RFID tag reader. The tag receives this signal and uses part of its energy to power the response.

The models shown in Figure 5 have a transmission range of a few meters, while other RFID tags are equipped with a battery and operate as a beacon that can broadcast information at all times. This type of RFID tag usually has a range of a few hundred meters. Unlike the bar code, RFID relies on radio-frequency; therefore, does not require line of sight to work.

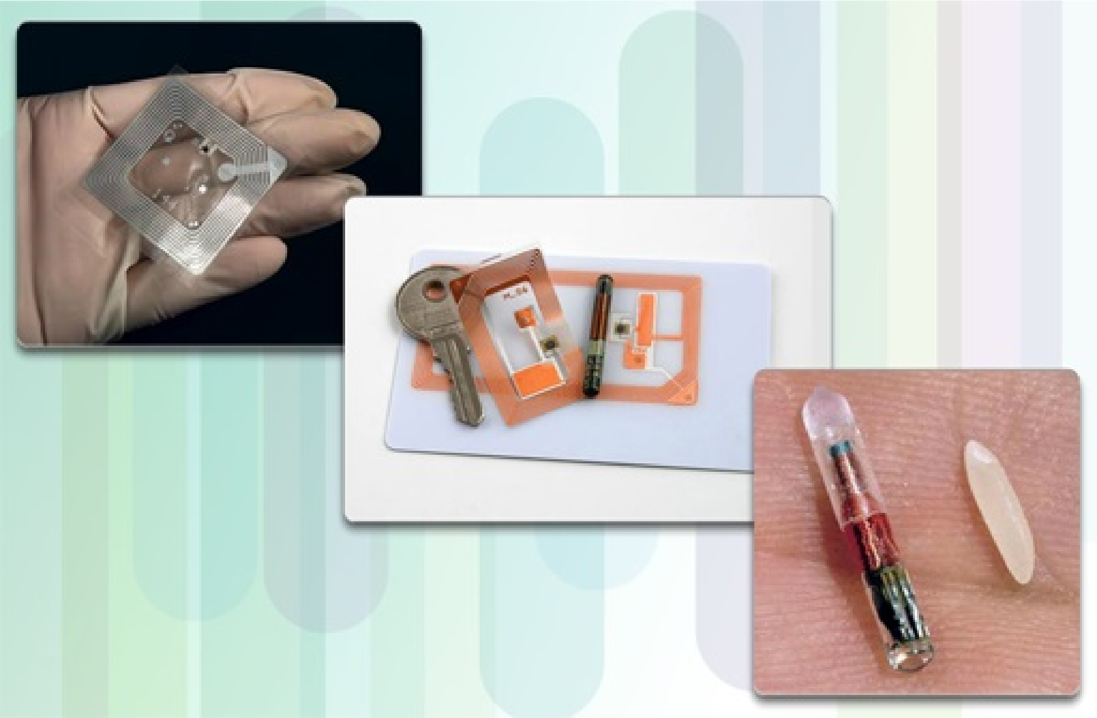


Figure 5 RFID devices

Because of its flexibility and low power requirements, RFID tags are a great way to connect a non-computer device to an IoE solution by providing information to an RFID reader device. For example, it is now common to find car factories attaching RFID tags to the car bodies. This allows for better tracking of that car throughout the assembly line.

The first generation of RFID tags is 'write once read many'. This means that they can be programmed in the factory once, but cannot be modified out in the field. Newer RFID tags are 'write many read many', with integrated circuits that can last 40 to 50 years and be written to over 100,000 times. These tags can effectively store an entire history of the asset to which they are attached, such as the date of manufacture, location tracking history, multiple service cycle, and ownership.

2.1.7 Controller

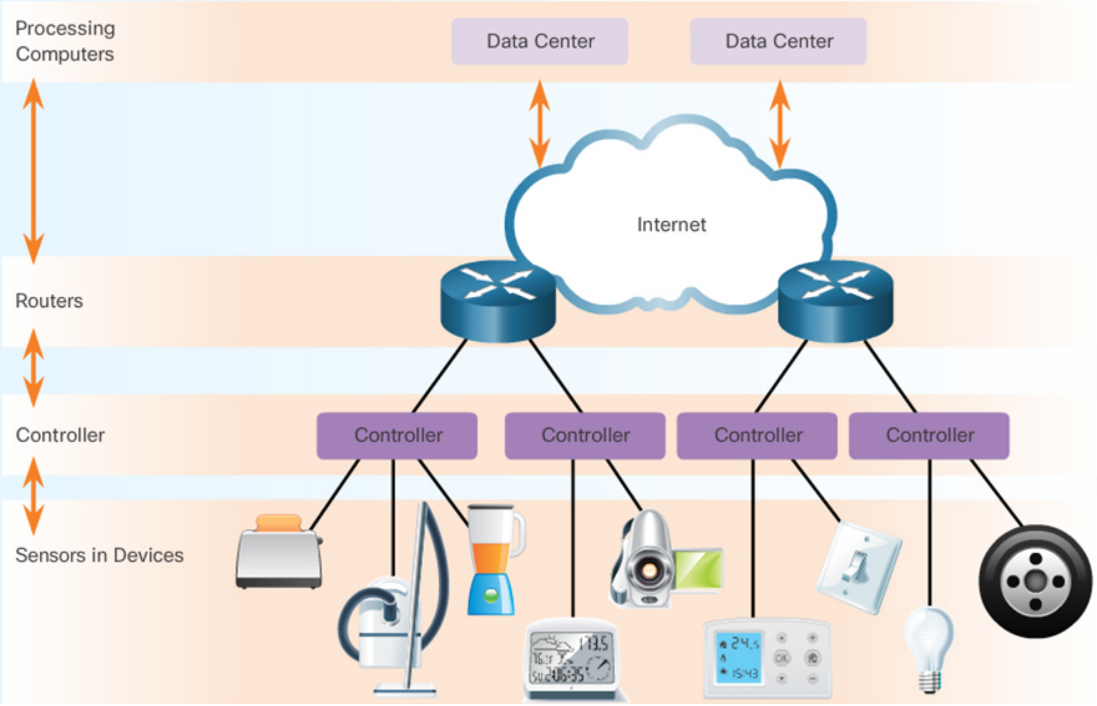


Figure 6 Controllers

Sensors can be programmed to take measurements, translate that data into signals, and then send that data to a main device called the controller. The controller is responsible for collecting data from sensors and providing an internet connection. 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.

In order to reach the internet and then the more powerful computers in the data centre shown in the figure, the controller will first send data to a local router. This router interfaces between the local network and internet and can forward data between them..

2.1.8 The IoT and the IoE

Video content is not available in this format.

In the video, Jim Grubb, Cisco's Chief Demonstration Officer, and John Chambers, Cisco’s former CEO, during the Cisco Live 2013 keynote demonstration, define the opportunity presented by the internet of things and how the internet of esverything will take advantage of these new opportunities.

The internet of everything is the networked connection of people, process, data and things.

In the video, the IoT is described as a market transition that is taking advantage of the reduced cost in connecting things to the Internet. As a result, the IoT implies a fundamental shift in the state of our present economy as we move towards connecting 50 billion devices by 2020.

However, the IoT is only one of several market transitions that are enabling the full potential of the IoE. For example, the following are transitions that are also enabling the IoE’s full potential:

- **mobility** − providing access to resources from any device, at any time, and from any place
- **cloud computing** − providing distributed computing resources and services over a network
- **big data** − as the volume of data being produced is accelerating, so too is our capacity to analyse and process it
- **IPv6** − expanding the current internet address space by 3.4×10^38 addresses, easily accommodating 50 billion devices by 2020, and billions upon billions more.

The amount of value an organisation derives from IoE depends on its ability to capture transitions, such as cloud, mobility, and the IoT. For example, John highlights Smart Grid, a solution that realises the benefit of the IoE by improving energy efficiency on the electricity grid provided by utilities and where the energy is used in homes and offices.

IoT is about how to connect the unconnected, making things accessible by the internet. As it relates to IoT, IoE is addressing why we are connecting the unconnected.

2.2 Data as a pillar

Data is a key element of all computer systems – from early computing to current systems. A predominant reason for having computer systems, has been to process and transmit data. In this section, you will learn how this is accomplished and what systems are used to convert digital data into human understandable terms.

2.2.1 What is data?

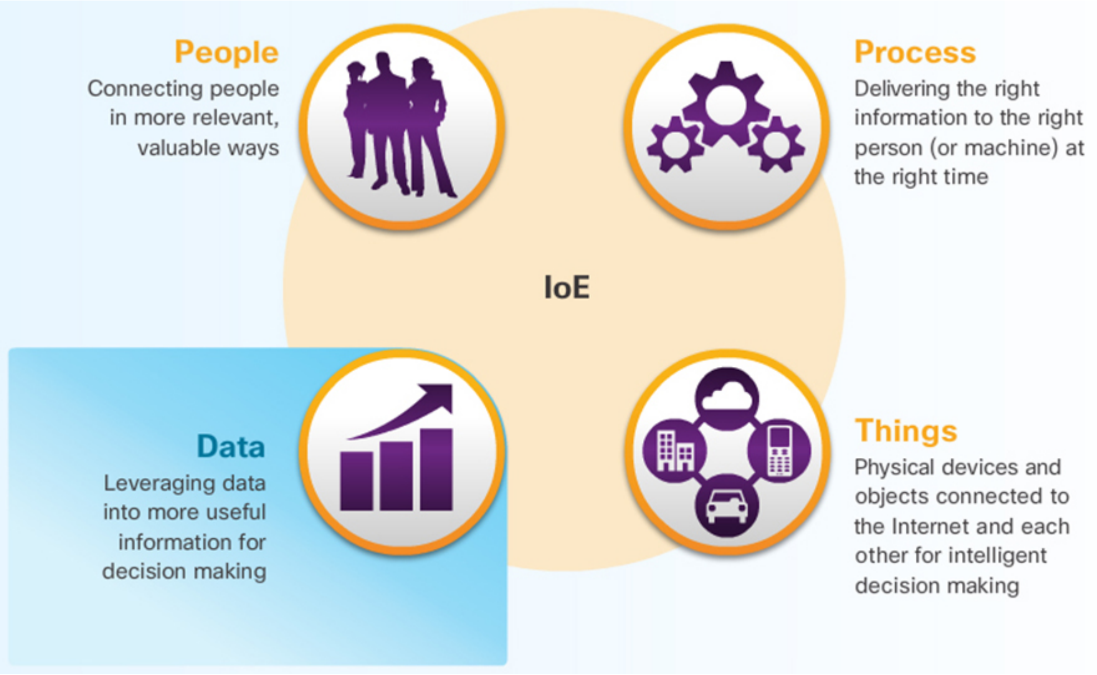

People
Connecting people in more relevant, valuable ways
Process
Delivering the right information to the right person (or machine) at the right time
IoE
Data
Leveraging data into more useful information for decision making
Things
Physical devices and objects connected to the Internet and each other for intelligent decision making

Figure 7 The four pillars: data

Data is a value assigned to anything that is around us. Data is everywhere. However, by itself, data can be rather meaningless. As we interpret the data, for example, by correlating or comparing, it becomes more useful. This useful data is now information. As this information is applied or understood it then becomes knowledge.

In electronic communication, data is represented as 1s and 0s. These discrete elements are known as bits (or binary digits). All electronic data is stored in this digital binary format. Whereas humans interpret words and pictures, computers interpret bit patterns.

A number of website provide free tools so you can see how letters are translated into binary code. You can try this out.

The advantage of using digital coding is that it can be stored more efficiently and can be transmitted over long distances without the quality becoming degraded.

2.2.2 Management of data

Computers generally lack the contextual awareness and intuitiveness of humans. As a result it is important to consider the following two states of data: structured and unstructured.

Structured data

Structured data refers to data that is entered and maintained in fixed fields within a file or record. Structured data is easily entered, classified, queried, and analysed by a computer. For example, when you submit your name, address, and billing information to a website, you are creating structured data. The structure will force a certain format for entering the data to minimise errors and make it easier for a computer to interpret it. Figure 8 represents different types of data being stored in specified locations so that computer programs can then locate the data.

Interactive content is not available in this format.
Figure 8 Locating data

Unstructured data

Unstructured data lacks the organisation found in structured data. Unstructured data is raw data. It does not possess the scaffolding that identifies the value of the data. Unstructured data lacks a set way of entering or grouping the data, and then analysing the data. Examples of unstructured data include the content of photos, audio and video files.

Structured and unstructured data are valuable assets to individuals, organisations, industries, and governments. Like other assets, the information gathered from both structured and unstructured data has measurable value. However, the value of that data can increase or decrease depending on how that data is managed. Even the best data loses value over time.

It is important for organisations to take all forms of data (structured, unstructured, and semi-structured) and determine ways to format that data so it can be managed and analysed.

To understand the management of data, it is important to understand concepts such as data storage and the transportation of data.

2.2.3 Data storage

When referring to storage space, we use the term bytes (B). A single byte is a combination of 8 bits. Other measurements include:

- **kilobytes (KB)** − approximately one thousand (10^3) bytes
- **megabytes (MB)** − approximately one million (10^6) bytes
- **gigabytes (GB)** − approximately one billion (10^9) bytes
- **terabytes (TB)** − approximately one trillion (10^12) bytes
- **petabytes (PB)** − approximately one quadrillion (10^15) bytes
- **exabytes (EB)** − approximately one quintillion (10^18) bytes.

If you have never seen this symbol before ^ it is a common shorthand for a mathematical power. A power is a number that is multiplied by itself a number of times. For example 10 *to the power of 2 (10^2) is 10*10 which is 100, again 10 to the power of 4 (10^4) is 10*10*10*10 or 10,000.*

Over the years, the amount of available storage space has increased exponentially. For example, not long ago the storage space of hard drives was typically measured in megabytes. Today, terabyte hard drives are common.

There are three primary types of data storage:

- **Local data** refers to data that is accessed directly, by local devices. Hard disks, USB flash drives, and CDs/DVDs are examples of local data storage. See Table 3 for more information.

Table 3 Types of local data storage

Optical drives	USB flash drives	Hard drives	External hard drives
An optical drive is used to write data onto a CD or DVD. These portable storage devices are inexpensive and easy to label and store.	USB flash drives are removable and rewritable. These portable storage devices can hold gigabytes of data.	Hard drives come pre-installed on most desktop or laptop computers. These devices store data on magnetic platters. They can store large amounts of data, 1 terabyte or more.	External hard drives that are enclosed in a case and are usually attached to your computer via a USB or Firewire port.

- **Centralised data** is stored and shared from a single centralised server. This information can be accessed remotely by multiple devices over the network or the internet. Using a centralised data server can result in bottlenecks and inefficiencies, and can become a single point of failure.
- **Distributed data** is managed by a central database management system (DBMS). 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 from the other sites. See Figure 9.

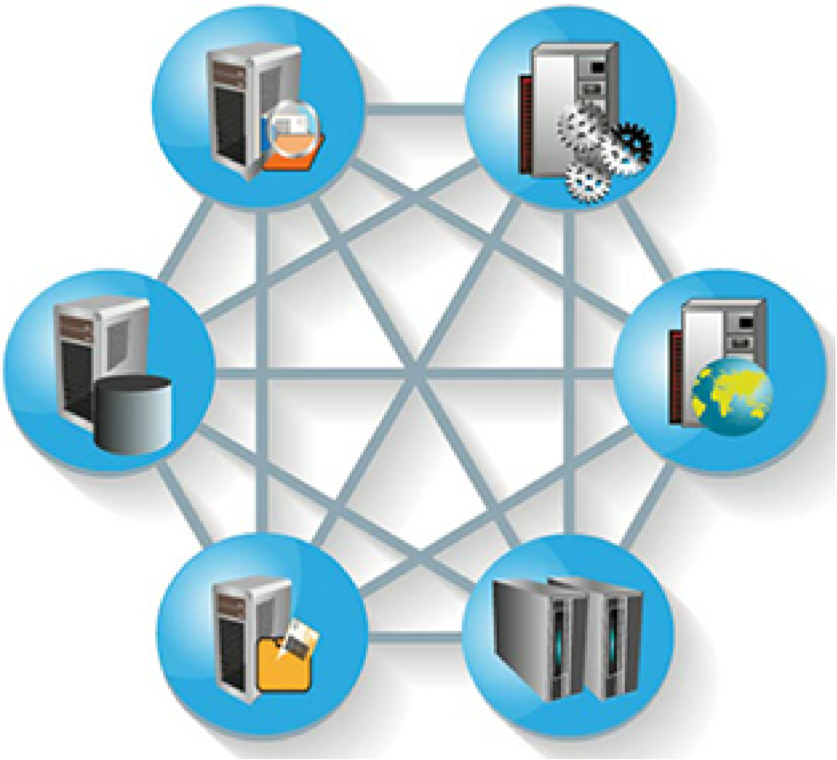


Figure 9 Distributed data

2.2.4 Internet service providers

In centralised and distributed data storage environments, data must be transported over the network or internet.

Devices that forward data across the internet must use an internet service provider (ISP). An ISP supplies the connections to allow internet access to individuals and businesses, and can also interconnect with other ISPs. Networks connect to an ISP at a point of presence (POP).

Within an ISP, a network of high-speed routers and switches move data between the various POPs. Multiple links interconnect the POPs to provide alternate routes for data in the event that one link fails or becomes overloaded with traffic.

To send information beyond the boundaries of an ISP network, packets are forwarded to other ISPs. As shown in the animation, the internet is made up of high-speed data links that interconnect multiple ISPs together. These interconnections are part of the very large, high-capacity network known as the internet backbone.

Video content is not available in this format.

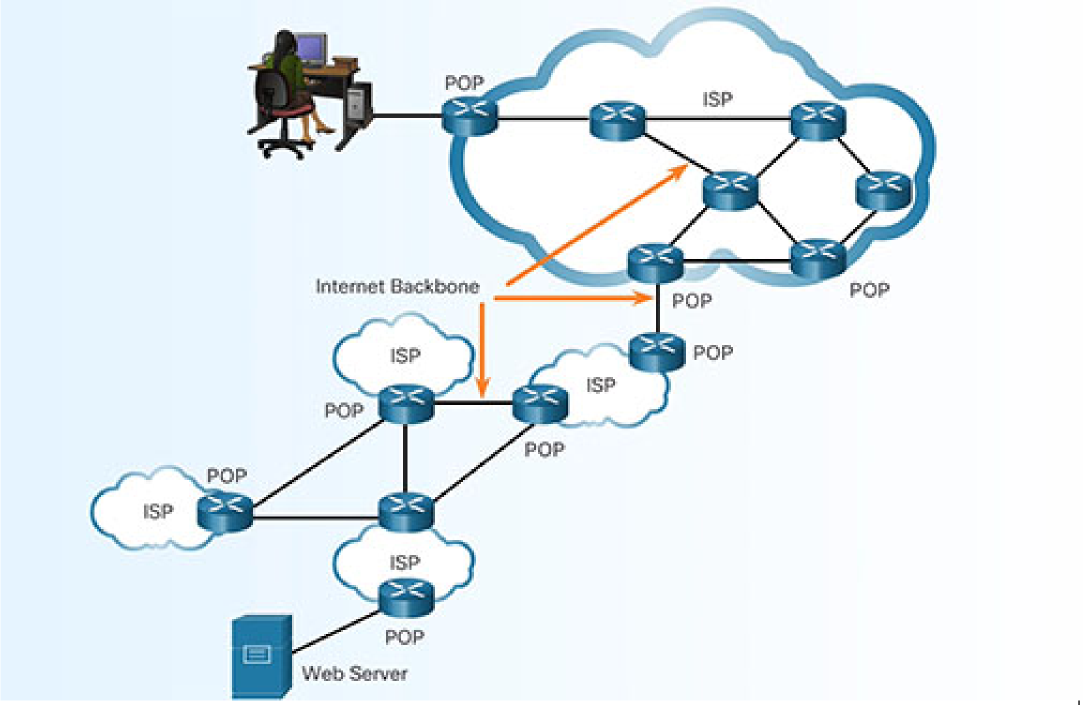


Figure 10 Internet service providers

2.2.5 IP addressing

Packets that cross the internet must be internet protocol (IP) packets. Each IP packet must contain a valid source and destination IP address. Without valid address information, packets will not reach the destination host and return packets will not make it back to the original source. The IP protocol defines the structure of the source and destination IP addresses. It specifies how these addresses are used in routing of packets from one host or network to another.

Currently, the internet uses IPv4 (IP version 4), but is transitioning to IPv6 (IP version 6). IPv6 allows for greater access and scalability with more available IP addresses and other features.

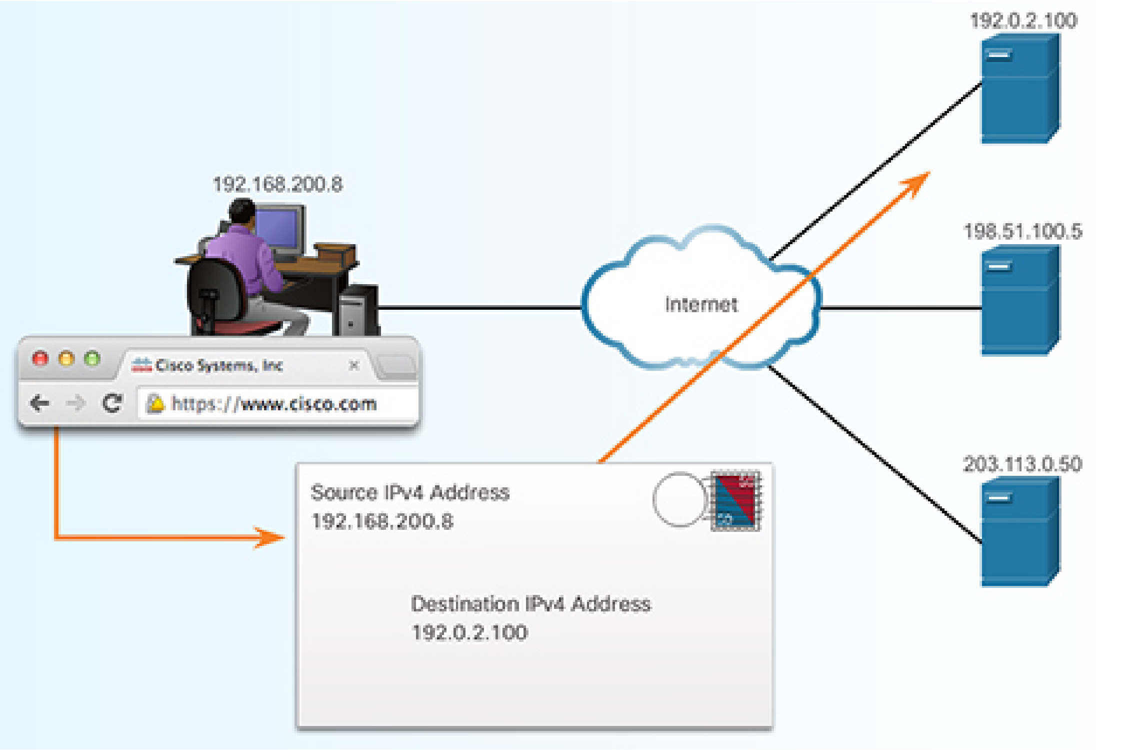


Figure 11 IP addressing

The IP address is similar to the mailing address of a person. It is known as a logical address because it is logically assigned based on the host location. This process is similar to the local government assigning a street address based on the logical description of the city, village, or neighborhood. It would be impossible to remember all of the IP addresses for all of the servers hosting services on the internet. Instead, there is an easier way to locate servers by associating a name with an IP address. In the figure, servers on the internet translate the name www.cisco.com to the IP address for the destination.

2.2.6 IP packets

Whether playing an internet video game, chatting with a friend, sending email, or searching the Web, the data being sent and received is carried in the form of IP packets. Before being sent on the internet, data is divided into IP packets. Packet size is between 64 to 1500 bytes for Ethernet networks. Downloading a single song that is 3 MB would require over 2000 packets of 1500 bytes each.

On networks, each byte of data is transmitted one bit at a time. Network bandwidth, or data transfer rate, is expressed in bits per second. For example, a one megabit (1,000,000 bits) connection means that data can be theoretically transmitted at one megabit per second (1 Mb/s).

2.2.7 IP address management

On the internet, each IP address must be unique. The Internet Assigned Numbers Authority (IANA) is responsible for controlling the distribution of IP addresses so that there is no duplication. IANA allocates blocks of IP addresses to one of five regional internet registries (RIRs). ISPs obtain blocks of IP addresses from the RIR in their geographic region. It is the responsibility of the ISPs to manage these addresses and assign them to customer networks and end users' devices and networks.

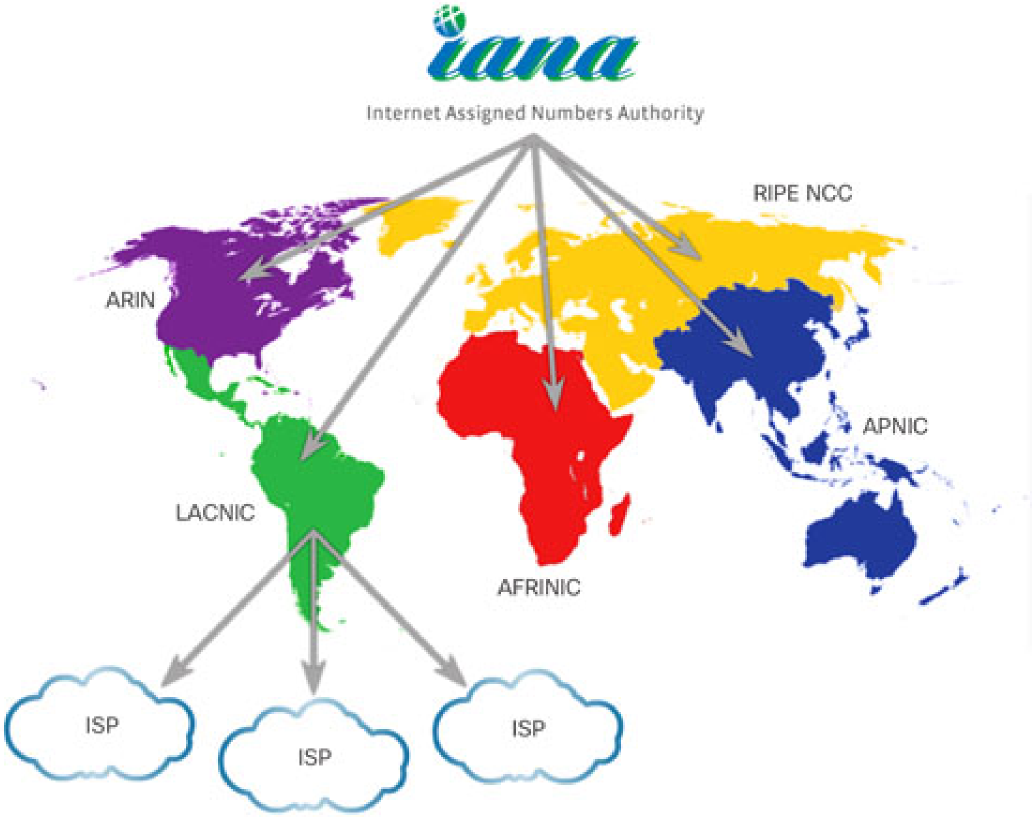


Figure 12 Regional internet registries: ARIN (USA, Canada); LACNIC (Latin America); AFRINIC (Africa); RIPE NCC (Europe and North Asia); APNIC (Southern Asia and the Pacific)

The ISP determines where to forward the traffic. Packets are passed from router to router, possibly through multiple ISP networks, until they reach their final destination. Routers in each of the ISPs use the destination address of the IP packets to choose the best path through the internet. The packet switching is transparent to the user, as they only see what was sent and received.

2.2.8 More connections equals more data

Why all the concern about data? Within the last decade, the volume of data that was produced in a year is now produced in a week. That amounts to over 20 exabytes of data produced a week. Data continues to grow exponentially as more of the unconnected become connected

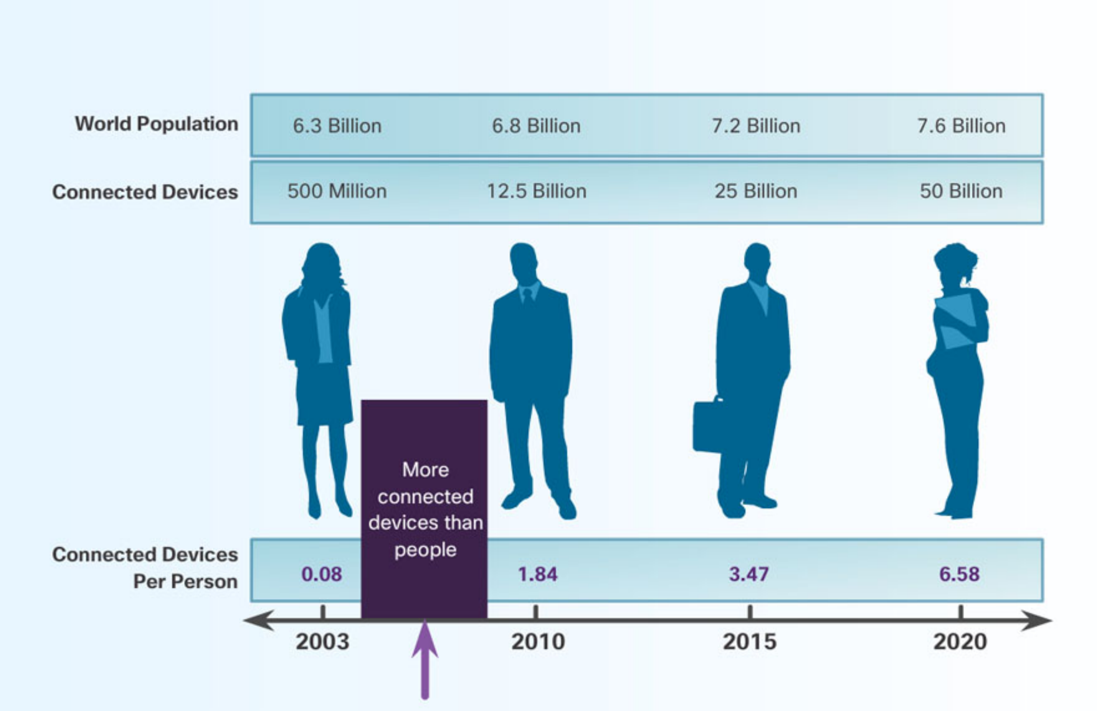


Figure 13 The time line illustrates that as time has progressed the number of connected devices has surpassed the world's population

2.2.9 Data in motion

Typically, data is viewed as information that has been collected over time. For example, it may have been collected through various transactions that represent an organisation's order-processing. This data has value to the organisation and is historical in nature. This is static data that we call 'data at rest'.

However, as the accelerated growth for large quantities of data continues, much of this data's value is lost almost as quickly as it is created. Devices, sensors, and video deliver this growing source of new data on a constant basis. This data provides maximum value while it is interacting in real-time. We call this 'data in motion'.

This influx of new data opportunities is providing new paths to improve our world, from solving global health issues to improving education. There is incredible potential for intelligent solutions to collect, manage, and evaluate data at the speed of human communications. As a result, the internet of everything will increasingly become about 'data in motion'. Watch Cisco's vision of bringing the evolution of data to the IoE.

Video content is not available in this format.

2.2.10 Managing big data

A driving factor of this growth of information is the number of devices connected to the internet, and the number of connections between those devices. But this is just the beginning. New devices are being connected to the internet daily, creating an abundance of new content.

With this amount of information, organisations must learn how to manage data and also, how to manage 'big data'.

There are three primary dimensions of big data that must be accounted for: volume, variety, and velocity.

Volume describes the amount of data being transported and stored. Variety describes the type of data it is. Velocity describes the rate at which this data is moving. Data cannot move without infrastructure. The swiftness of infrastructure (input/output, bandwidth, and latency) and the ability to rapidly enable optimal resources (network, CPU, memory and storage) directly affects the velocity of data.

2.2.11 Big data analytics

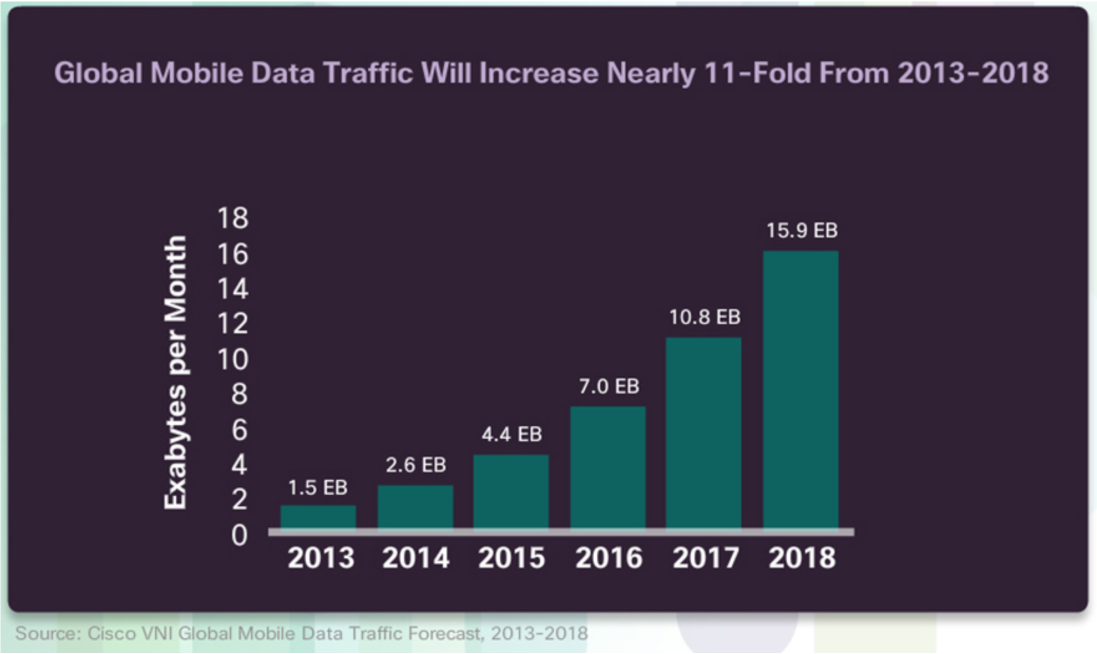


Figure 14 Global mobile data traffic growth/top-line

Big data applications receive information from a wide array of data sources, including PCs, smartphones, tablets, machines, sensors, social media, and multimedia applications. Much of this growth in data is due to mobile devices, as shown in the figure. Mobility enables anytime, anywhere, any device, and any content-user engagement.

Big data refers to the way in which organisations collect and analyse vast stores of data for insights that can help identify trends, predict behaviour, and empower decision makers. It considers:

- how much data is generated
- how this data is identified and managed as an asset to the organisation
- how this data is turned into usable information
- how organisations use this data to make decisions.

Ask yourself, what happens when we share information or an opinion about a business on a social network? How is this information propagated? Who gets this information? And more importantly, how are businesses reacting and using this information to create new customer connections?

2.2.12 Big data analytics (cont.)

Video content is not available in this format.

Big data applications must be able to gather this data and structure it in a way that can create value for organisations. For example, big data applications must account for changing data sources and trends, such as:

- **mobility** − mobile devices, events, sharing, and sensor integration
- **data access and consumption** − internet, interconnected systems, social networking, and access models
- **ecosystem capabilities** − major changes in the information processing model and the availability of an open source framework

As a result, the cost and complexity of these models has increased, prompting changes in the way big data is stored, analysed, and accessed. Organisations must adjust their current data models to accommodate big data. As a result, organisations are increasingly using virtualisation and cloud computing to support their big data needs.

2.2.13 Virtualisation

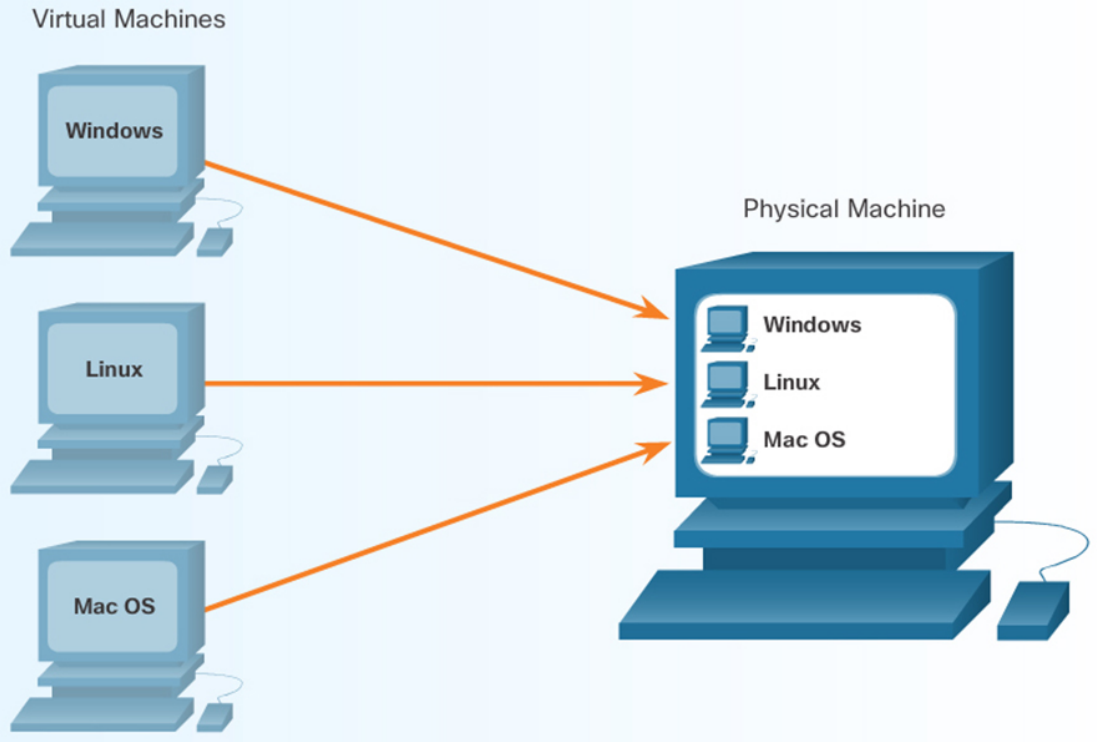


Figure 15 Virtual machines

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 virtualisation 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 virtualising 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 virtualisation 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.

2.2.14 Cloud computing

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 virtualisation to deliver their services. It can also reduce the operational costs by using resources more efficiently. These companies provide four distinct categories of services. The table below outlines each category in more detail

Table 4 Categories of cloud computing services

SaaS	PaaS	IaaS	ITaas
Software as a Service: Applications delivered over the web to the end users.	Platform as a Service: Tools and services used to deliver the applications.	Infastructure as a Service: Hardware and software to the power servers, storage, networks and operating systems.	IT as a Service: IT professionals support applications, platforms and infastructure.

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

2.2.15 Data centres

Data centres are a critical enabler of cloud computing. A data centre 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 because most organisations are dependent on their IT operations.

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

- **Location** – Data centres 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 centre should extend tight controls over physical access and on-site personnel.
- **Electrical** – There should be sufficient access to electrical power with 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 3000 data centres in the world that offer general hosting services (IaaS) to individuals and organisations. There are many more data centres that are owned and operated by private industries for their own use.

Watch the Youtube video for more information and a detailed tour of the Cisco Data Center in Allen, Texas.

2.2.16 Clouds

Cloud computing uses a shared pool of computing resources (e.g., networks, servers, storage, applications, and services) to provide on-demand network access. Using virtualisation in data centre environments, Cloud computing can be rapidly scaled with minimal management and effort.

The National Institute of Standards and Technology (NIST) has defined four types of cloud deployment models:

- private
- public
- community
- hybrid.

A private cloud is created exclusively for a single organisation. 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 organisation.

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 organisations 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 organisations 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 organisations in the community. The differences between public clouds and community clouds are the functional needs that have been customised for the community. For example, healthcare organisations must remain compliant with policies and laws (e.g., HIPAA) that require special authentication and confidentiality. Organisations 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 organisation 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.

2.2.17 Three critical cloud conversations

Cloud computing has already helped organisations make significant changes to their infrastructures. This process will become more pervasive as organisations take advantage of the IoE and assess big data needs. Organisations must leverage a variety of clouds. They will need an infrastructure and IT staff able to blend those clouds, and they will need to determine which cloud model might be best for each service.

Table 5 Clouds

The IoE requires a variety of cloud models	All cloud models must work together seamlessly	Enterprises must keep their options open
Organisations need maximum flexibility to efficiently and reliably connect people and things: • private • public • community • hybrid.	When selecting cloud solution providers, integration and consistency across all models is a critical factor.	The IoE is an evolving marketplace and organisations must evolve with it.
	Cloud solution providers must offer: • security • compliance • performance.	Choice is critical Avoid getting locked in to one provider or one methodology. Need expert advice to capitalise on the evolution of the cloud.
Organisations need a flexible infrastructure that: • adapts • speeds service introduction • ensures governance and financial reporting for each model.		

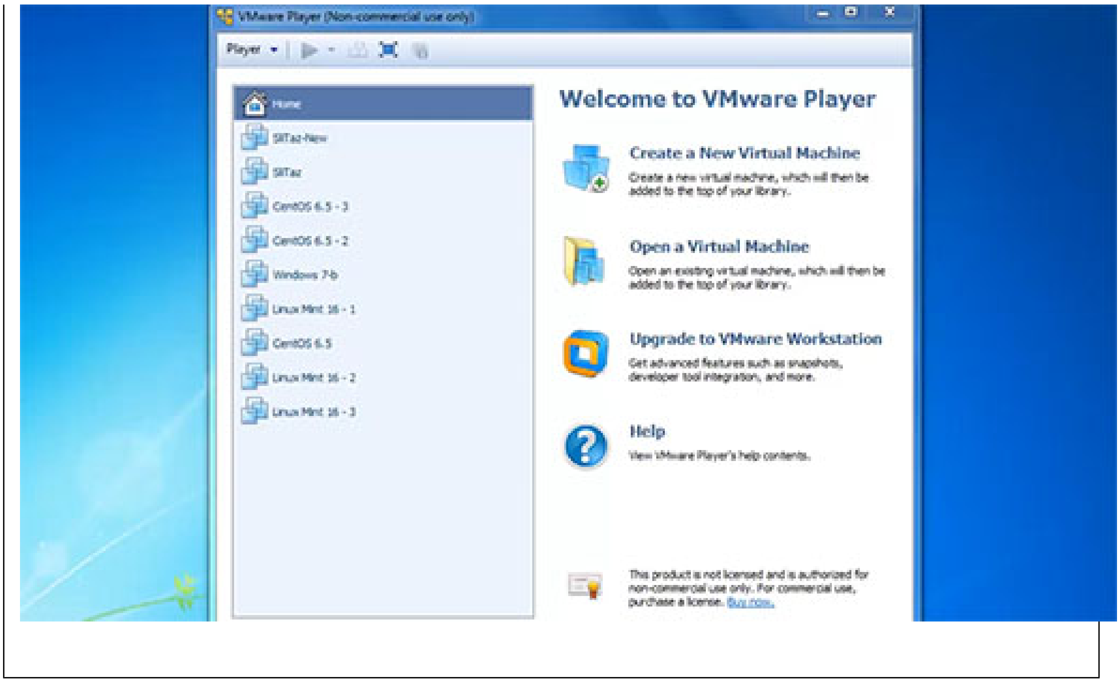
2.2.18 Lab: install a Linux virtual machine (optional)

Virtualisation is a critical factor in cloud computing and data centres. You can experience virtualisation on your own PC by installing a virtual computer.

Virtual computers that run within a physical computer system are called virtual machines. Today, entire computer networks are virtualised. Anyone with a modern computer and operating system has the ability to run virtual machines from the desktop.

Watch a demonstration of installing a Linux virtual machine.

Video content is not available in this format.



Welcome to VMware Player

Create a New Virtual Machine

Create a new virtual machine, which will then be added to the top of your library.

Open a Virtual Machine

Open an existing virtual machine, which will then be added to the top of your library.

Upgrade to VMware Workstation

Get advanced features such as snapshots, developer tool integration, and more.

Help

View VMware Player's help contents.

This product is not licensed and is authorized for non-commercial use only. For commercial use, purchase a license. Buy now.

The video demonstration shows how to complete this activity. After viewing the video, you can download the Lab – Install a Linux Virtual Machine (Optional) document to investigate the activity on your own.

Please be aware that virtualisation and running a Linux Virtual Machine will not work on all computers and devices being used to read this course. This optional activity is designed for desktop virtualisation using a personal computer. Another challenge you must be aware of before you commence is that virtualisation requires extra computer system memory which your own system may not have. If you have at least 2Gb (gigabytes) of memory (RAM) available this activity will work.

An alternative solution, if you have sufficient bandwidth on your internet connection, is to use SuseStudio. While this is advanced, it does allow you to run a remote Linux desktop system.

Another alternative is to use the web browser friendly demo version of Linux Unhatched from NDG who also work in partnership with Cisco Systems. You will need to sign in and you will be able to use Linux on any HTML5 compatible browser. This is unique as it is running on cloud based virtualisation.

2.3 People as a pillar

The reality is that we are all connected (like it or not) − the chances are as you are reading this course you may be connected to others via email, text (SMS) or social media. In this section you will learn about:how information adapts the way we behave, how (and why) businesses use data and the essential collaborative nature of the internet.

2.3.1 People must be connected

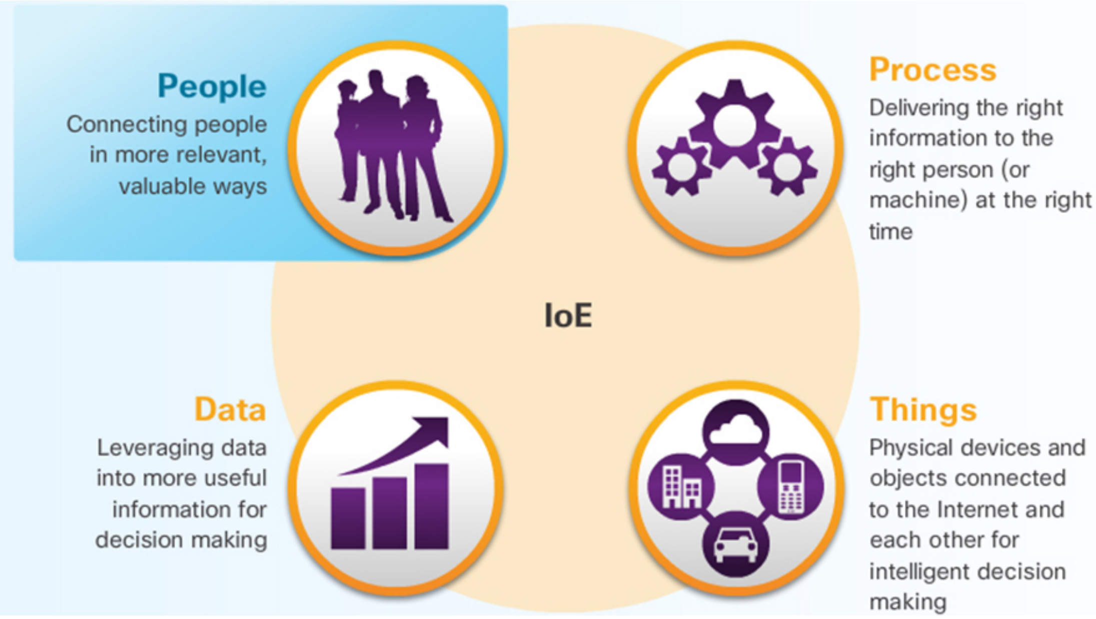

People
Connecting people in more relevant, valuable ways
Process
Delivering the right information to the right person (or machine) at the right time
IoE
Data
Leveraging data into more useful information for decision making
Things
Physical devices and objects connected to the Internet and each other for intelligent decision making

Figure 16 The four pillars: people

Data alone serves no purpose. A large amount of data which no one can access, serves no one. Organising that data and transforming it into useable information enables people to make better-informed decisions and take appropriate actions. This creates economic value in an economy that is enabled by the internet of everything.

This is why people is one of the four pillars. People are a central figure to any economic system. People interact as producers and consumers where the intent is to improve well-being by satisfying human needs. Whether the connections are people-to-people (P2P), machine-to-people (M2P), or machine-to-machine (M2M), all connections, and the data generated from those connections, are used to enhance the value for people.

The internet is teeming with data. Having access to the data and then taking action based upon the knowledge gained from this information is what the IoE is all about. For example, when Jack Andraka was a 15 year old high school student, he accessed information on the internet to develop a test that could detect pancreatic cancer at a much earlier stage when chances for survival are significantly better.

What would you do to make your world a better place?

2.3.2 Information transforms behaviour

> This [the IoE] is not about technology at all. It's about how we change people's lives.
>
> John Chambers, former CEO Cisco Systems

Value is a measure of benefit in an economic system. It is people who determine the value of offerings through a system of exchange. It is important to highlight that while data and analytics matter, it is judgement from people that turns data into insights, and insights into IoE value.

The IoE enables accurate and timely information that can result in changing human behaviour for the benefit of all people. It facilitates feedback that allows people to make informed decisions that bridge the differences between actual outputs and desired outputs. This is known as a feedback loop. A feedback loop can provide real-time information based on current behaviour, and then deliver actionable information to modify that behaviour.

2.3.3 How businesses use data

The feedback loop is an important asset to businesses because it helps them react and plan in a constantly changing business landscape. It allows a business to have relevant and competitive offerings that address customer needs. For example, many retailers use loyalty cards to track customer purchases and identify trends. This enables retailers to promote offerings directly to the most relevant shoppers that represent the greatest potential for profit.

A hundred years ago businesses were focused on creating undifferentiated products, selling the same product to everyone. This was aligned with the evolution of mass production during the same time period. Equally aligned were promotional strategies for products, mass marketing using signage, pamphlets, and newspapers in hopes that people would buy the product.

However, a single business product or service is not likely to be needed by every person. A modern business is aware of targeted marketing that creates differentiated offerings based on customer needs. This is why businesses need access to customer data.

Micromarketing example

Target marketing is aimed at a specific group of people, separate from the market as a whole. This market may be based upon people who live in the same region, or have the same job title, or make a certain amount of money.

For instance, consumer data can show that a particular television programme is viewed most by people aged 40 to 65 with an annual household income of $250,000 or more. These programmes often run commercials for high-end cars because the car companies have access to the viewer data. They will pay for their commercials to run when their target market is most likely to see them.

Micromarketing is an even more precise version of marketing. E-commerce sites and loyalty programmes allow businesses to know more precisely what kind of product or service you may require.

For example, you may receive an email from an online site where you have purchased (or even browsed) before. This email may let you know about a sale on an item that is similar to something you have purchased in the past. Additionally, while browsing the web, you may notice an ad for the exact pair of shoes you were looking at online yesterday. This is not a coincidence.

Collaboration

It is through inclusive practices that enable people to contribute and collaborate effectively that better decisions will be made to maximise value. In fact, better collaboration within organisations is an area that will benefit most from the IoE. Collaboration will facilitate innovative new offerings that realise the potential of the IoE.

Collaboration in the IoE will make organisations more aware of customer needs and opportunities. Customers will be able to solve problems and get advice when and where it’s most convenient for them. Organisations will have new sources of information as people connect using data, voice, video, and social media.

Organisations using collaboration technologies will be able to predict and proactively resolve problems. They will be able to leverage social media to identify potential problems and resolve them before they become a serious issue. They will be able to identify and connect to the right expert at the right time. The expertise of highly-trained and knowledgeable employees will be more easily scaled across multiple locations.

With these collaboration technologies, businesses will experience the increased innovation and agility that will drive their growth. Organisations will be able to foster better relationships between employees who provide creative approaches to offerings, solutions, and processes. They will also be better able to connect decision makers, regardless of location, so that new innovations can be realised sooner.

2.4 Process as a pillar

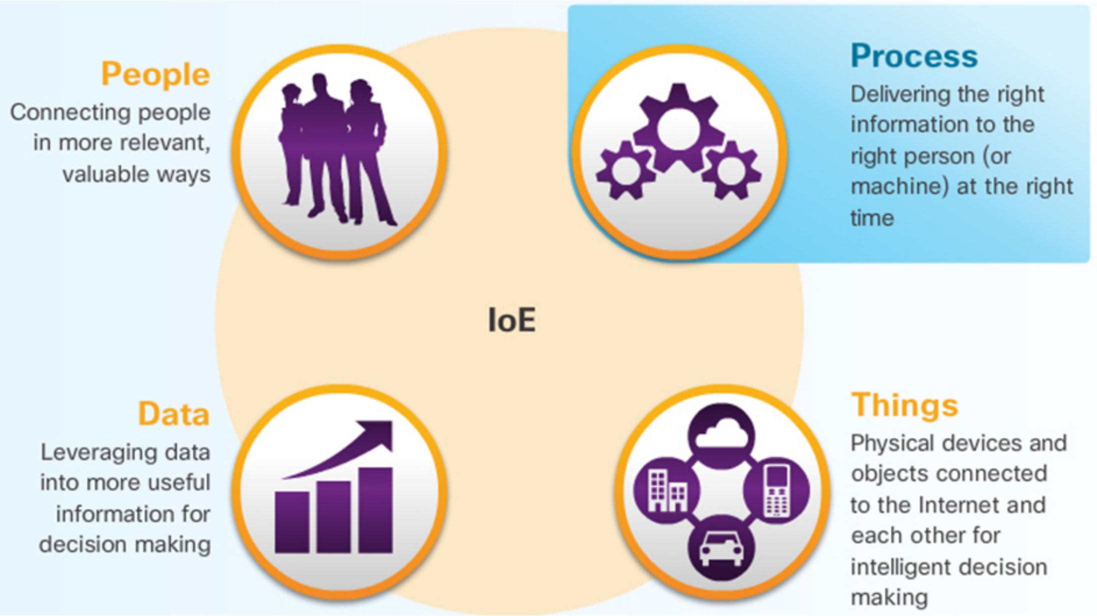

People
Connecting people in more relevant, valuable ways
Process
Delivering the right information to the right person (or machine) at the right time
IoE
Data
Leveraging data into more useful information for decision making
Things
Physical devices and objects connected to the Internet and each other for intelligent decision making

Figure 17 The four pillars: process

The fourth pillar is process. Processes play an important role in how the other pillars of things, data, and people work with each other to deliver value in the connected world of IoE.

The internet has revolutionised the way businesses manage their supply chains and the way consumers shop. Soon we will have visibility into processes we could never see before. This will provide opportunities to make these interactions faster and simpler.

With the correct process, connections become relevant and add value because the right information is delivered to the right person, at the right time, in the appropriate way.

Processes are facilitating interactions between people, things, and data. Today, the IoE brings them all together by combining machine-to-machine (M2M), machine-to-people (M2P), and people-to-people (P2P) connections, as shown in Figure 18.

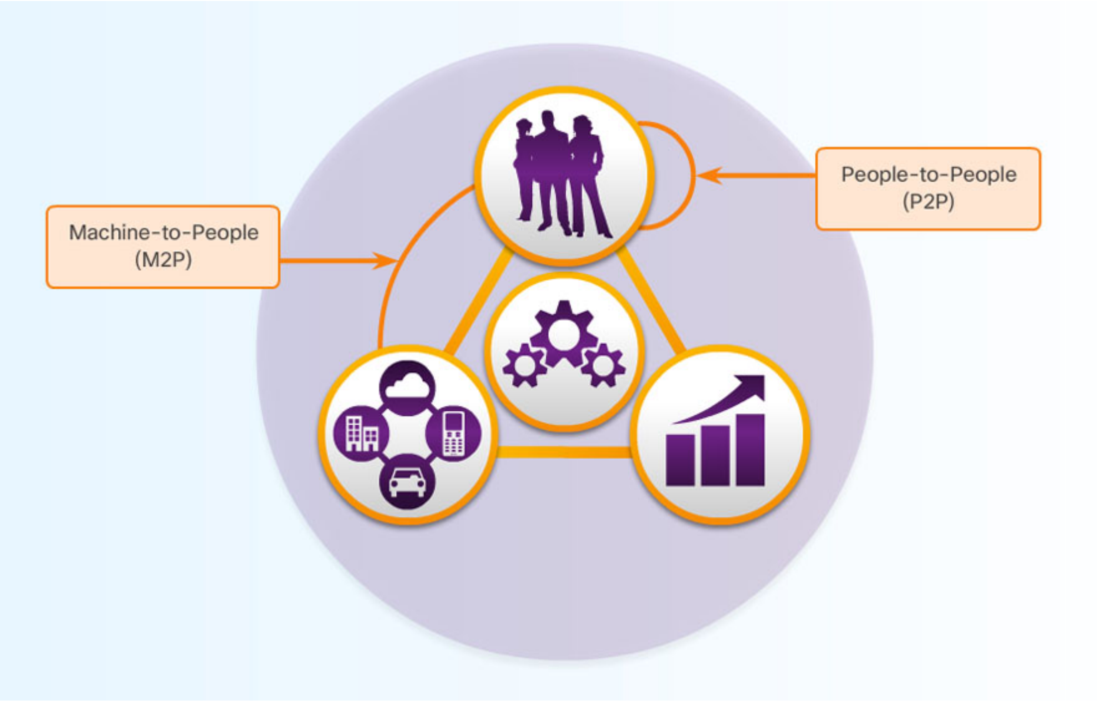


Figure 18 The IoE combines machine-to-machine (M2M), machine-to-people (M2P), and people-to-people (P2P) connections

2.4.1 M2M connections

Machine-to-machine (M2M) connections occur when data is transferred from one machine or 'thing' to another over a network. Machines include sensors, robots, computers, and mobile devices. These M2M connections are often called the internet of things.

An example of M2M is a connected automobile that is signaling that a driver is almost home, which prompts the home network to adjust the home temperature and lighting.

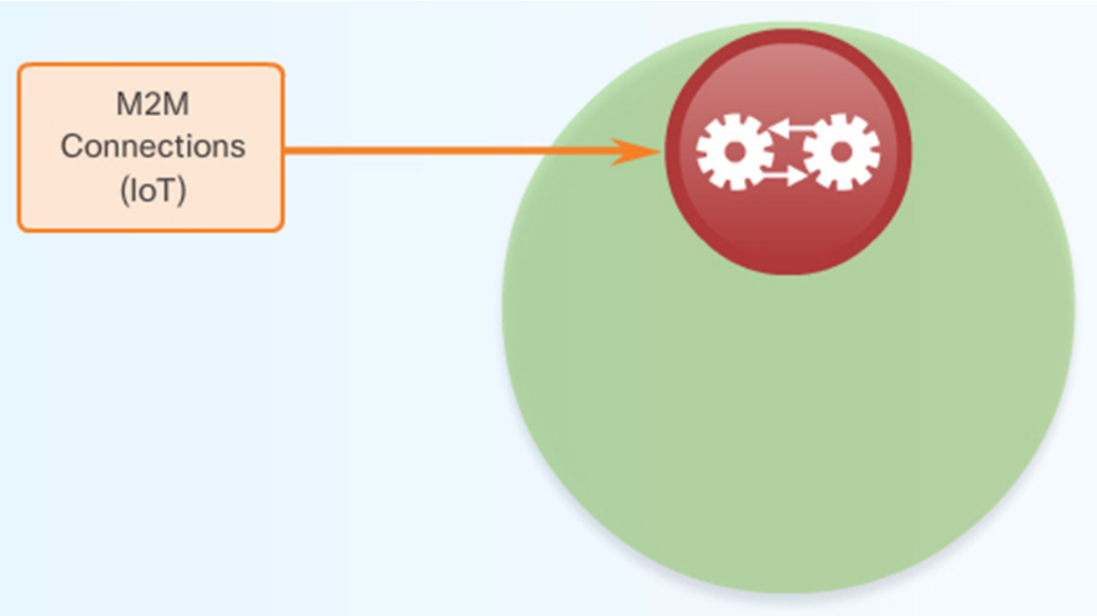


Figure 19 M2M connections within the IoT

2.4.2 M2P connections

Machine-to-people (M2P) connections occur when information is transferred between a machine (such as a computer, mobile device, or digital sign) and a person, as shown in Figure 20. Whether a person gets information from a database, or conducts a complex analysis, this is an M2P connection. These M2P connections facilitate the movement, manipulation, and reporting of data from machines to help people make informed judgments. The actions that people take based on their informed judgments complete an IoE feedback loop.

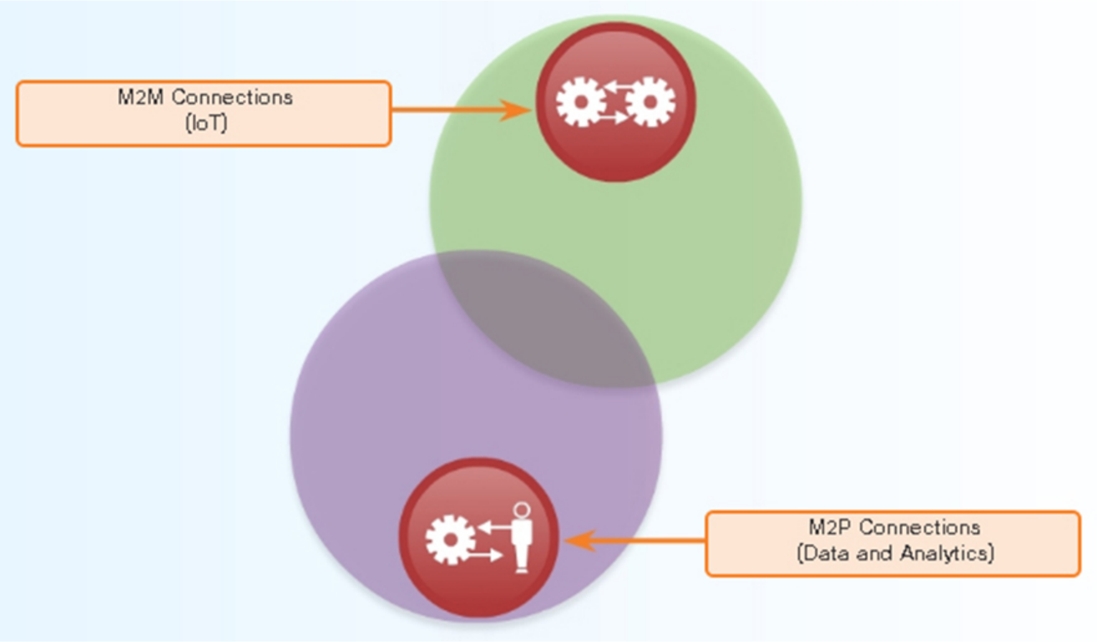
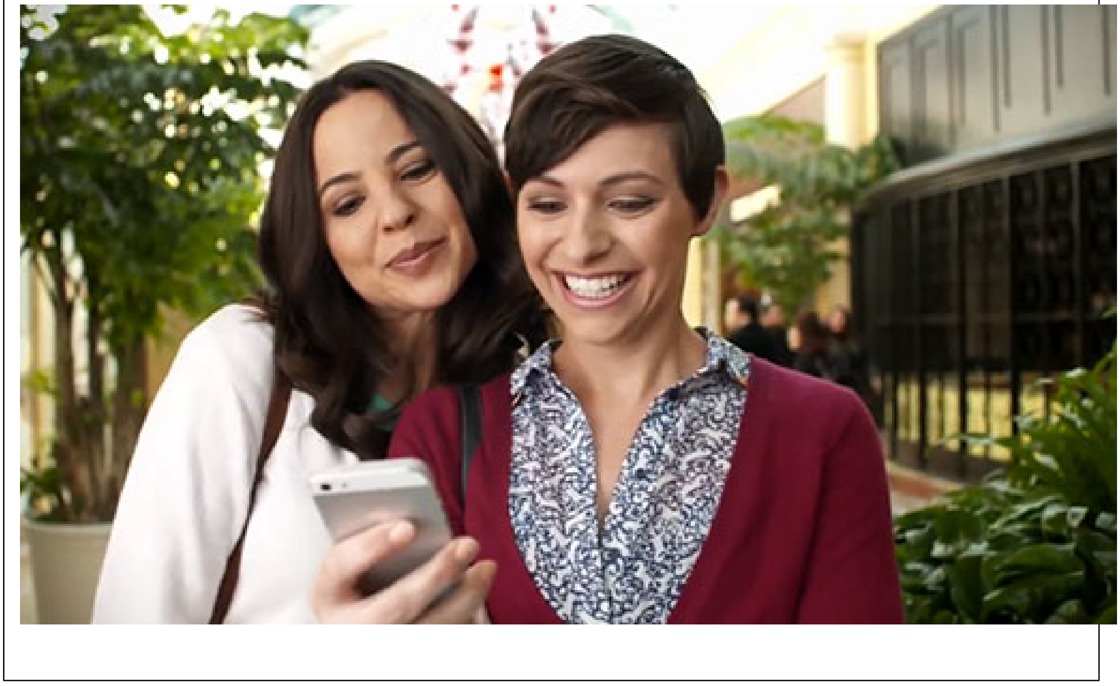


Figure 20 Interactions between M2M and M2P connections.

Watch the video of examples of M2P connections.

Video content is not available in this format.



2.4.3 P2P connections

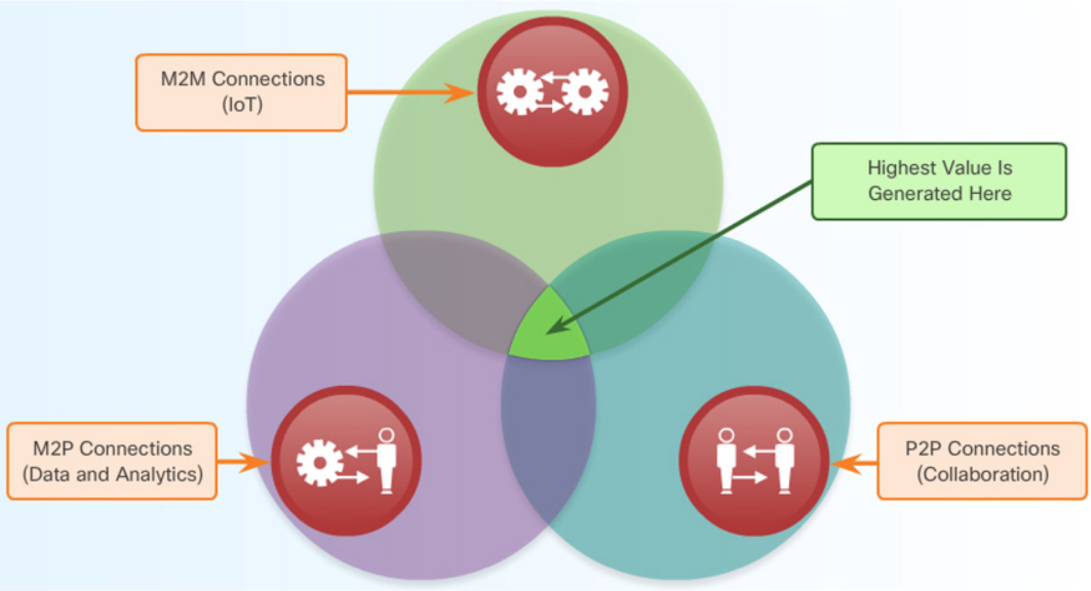


Figure 21 Venn diagram of P2P, M2P and M2M connections

People-to-People (P2P) connections occur when information is transferred from one person to another. Increasingly, P2P connections happen through video, mobile devices, and social networks. These P2P connections are often called Collaboration.

As shown in the figure, the highest value of the IoE is realised when process facilitates the integration of M2M, M2P, and P2P connections.

2.4.4 Property management case study

In what ways can the combination of people, process, data, and things across a secure platform create value? Consider property management and owners, as shown in the Table 6.

Table 6 Combined value of the three connections, M2M, M2P, and P2P.

Connection type	Value of combined connections
95,000 sensors and devices connected to Cisco network, including fire alarms, wireless access points, video surveillance cameras, temperature sensors, and HVAC	Cut energy costs 21% in 2012, another 11% in 2013
Data from sensors and devices monitored by building managers with mobile devices	Providing network connectivity to tenants
Energy consumption analysed in real time to increase efficiency, optimise usage	
Mobile employees work with tenants and respond to service request in real time via mobile devices	Plans to offer integrated unified communications (UC), wireless, physical security services

In a commercial real estate market, a property management company must look for ways to differentiate itself from its competitors by providing unique services to tenants and increasing revenues along the way.

In one example, a property management company installed 95,000 sensors throughout the building on a Cisco network to track energy usage. By applying analytics applications, the company was able to track energy usage and help tenants lower their energy bills. This company also provided their building managers and other facilities employees with mobile devices to improve collaboration and service to tenants.

The result was a 21% reduction in energy costs in 2012.

2.4.5 Timely and relevant information

THE INTERNET OF EVERYTHING
What will the world look like when we connect the unconnected?
Empowered
Vibrant
Intelligent
Relevant
Innovative
In an interconnected world, even the smallest things will have big implications.
TAKE, FOR EXAMPLE,
A DROP OF WATER.

Figure 22 The internet of everything

The billions of M2M, M2P, and P2P connections make possible the 'everything' in the IoE. The process pillar leverages the connections between data, things, and people to deliver the right information, to the right thing or person, at the right time. It is these billions of connections that add value.

A drop of water is a great metaphor for the IoE. A single drop by itself is not that significant. Yet, when combined with millions or even billions of other drops, it can change the face of our planet. Like a single drop of water, a single person, bit of data, or thing connected with billions of other people, data, and things can shape the face of our planet.

To convert our metaphor into a 'real-world' IoE example, consider how one tiny drop of water can begin a chain reaction that causes a big result. Monitoring systems send alerts of a sudden thundershower. Sensors talk to networks. Networks talk to traffic grids. Traffic grids talk to energy systems. All these work in concert to protect people and preserve their quality of life.

A drop of water

Environmental sensors detect an upcoming rain, and relay that information to the organisational network managing that area. Everyone involved in that network within the impacted timeframe is informed of the unexpected weather shift, and schedules are adjusted automatically.

A construction company's connected network shifts labour schedules and material deliveries to continue production within safe areas. soccer practices are cancelled and business meetings in outdoor venues are rescheduled indoors

Environmental sensors detect an upcoming rain, and relay that information to the organizational network managing that area. Everyone involved in that network within the impacted timeframe is informed of the unexpected weather shift, and schedules are adjusted automatically.

A CONSTRUCTION COMPANY'S CONNECTED NETWORK SHIFTS LABOR SCHEDULES AND MATERIAL DELIVERIES TO CONTINUE PRODUCTION WITHIN SAFE AREAS. SOCCER PRACTICES ARE CANCELLED AND BUSINESS MEETINGS IN OUTDOOR VENUES ARE RESCHEDULED INDOORS.

Figure 23a

Transportation systems work in congruence to resolve traffic risks due to rain. Road sensors detect the change and initiate dispersion of water-resistant solutions to the roads to mitigate road slickness. The lighting network updates to turn on appropriate lights for increased visibility.

Traffic grids work together to optimise traffic flow that accounts for adjusted driving patterns based on behaviour trends.

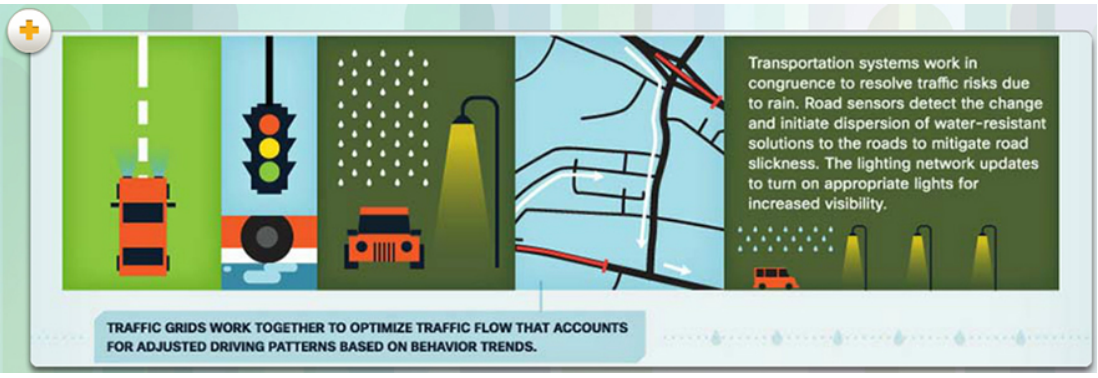

Transportation systems work in congruence to resolve traffic risks due to rain. Road sensors detect the change and initiate dispersion of water-resistant solutions to the roads to mitigate road slickness. The lighting network updates to turn on appropriate lights for increased visibility.
TRAFFIC GRIDS WORK TOGETHER TO OPTIMIZE TRAFFIC FLOW THAT ACCOUNTS FOR ADJUSTED DRIVING PATTERNS BASED ON BEHAVIOR TRENDS.

Figure 23b

Agricultural systems connected to a weather monitoring system receive information about a weather pattern change. The agricultural system makes real-time adjustments to the water system to optimise irrigation and keep proper soil moisture levels, while minimising the risk of crop destruction due to overwatering.

Sensors on a fruit tree's branches detect the amount of sag and alert a farmer to projected yield.

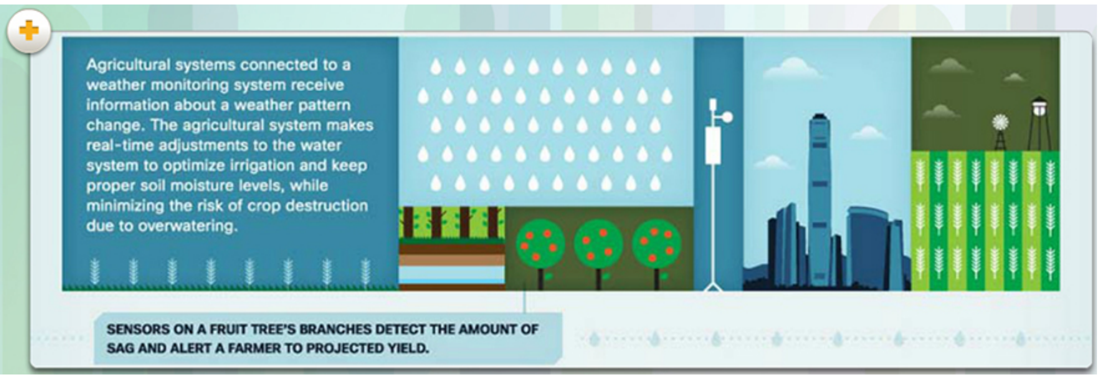

Agricultural systems connected to a weather monitoring system receive information about a weather pattern change. The agricultural system makes real-time adjustments to the water system to optimize irrigation and keep proper soil moisture levels, while minimizing the risk of crop destruction due to overwatering.
SENSORS ON A FRUIT TREE'S BRANCHES DETECT THE AMOUNT OF SAG AND ALERT A FARMER TO PROJECTED YIELD.

Figure 23c

The internet of everything will enhance our lives tremendously, as even one unassuming element will have sweeping implications for business, social interactions, and well-being in general. Amazing things will happen, and amazing experiences will be created.

The Internet of Everything will enhance our lives tremendously, as even one unassuming element will have sweeping implications for business, social interactions, and well-being in general. Amazing things will happen, and amazing experiences will be created.

Figure 23d

2.5 Terms and concepts practice

This activity will help you to test some of the terms and concepts you've been introduced to.

ISP

IANA

data velocity

!Warning! OpenSans not supportedvirtualisation

!Warning! OpenSans not supportedcloud computing

!Warning! OpenSans not supportedM2M

!Warning! OpenSans not supportedfeedback loop

!Warning! OpenSans not supportedRFID tag

!Warning! OpenSans not supportedbig data

Match each of the items above to an item below.

internet service provider

the organisation that oversees the assignment of internet addresses

the rate at which data moves on the network infrastructure

!Warning! OpenSans not supportedallows a computer to run multiple operating systems and programs at the same time

!Warning! OpenSans not supporteduses shared virtualised computing and network resources to deliver IT services across the internet

!Warning! OpenSans not supportedthings communicating with other devices

!Warning! OpenSans not supportedallows people to make informed decisions that bridge the differences between actual outputs and desired outputs

!Warning! OpenSans not supportedan active or passive device that provides identification information when in the presence of a reader device

!Warning! OpenSans not supportedrefers to the way in which organisations collect and analyse vast stores of data for insights that identify trends, predict behaviour, and empower decision makers

2.6 Session 2 quiz

Check what you have learned in Session 2.

Session 2 quiz

Use 'ctrl' (cmd on a Mac) or right-click to open the quiz in a new window or tab then come back here when you're finished.

2.7 Summary

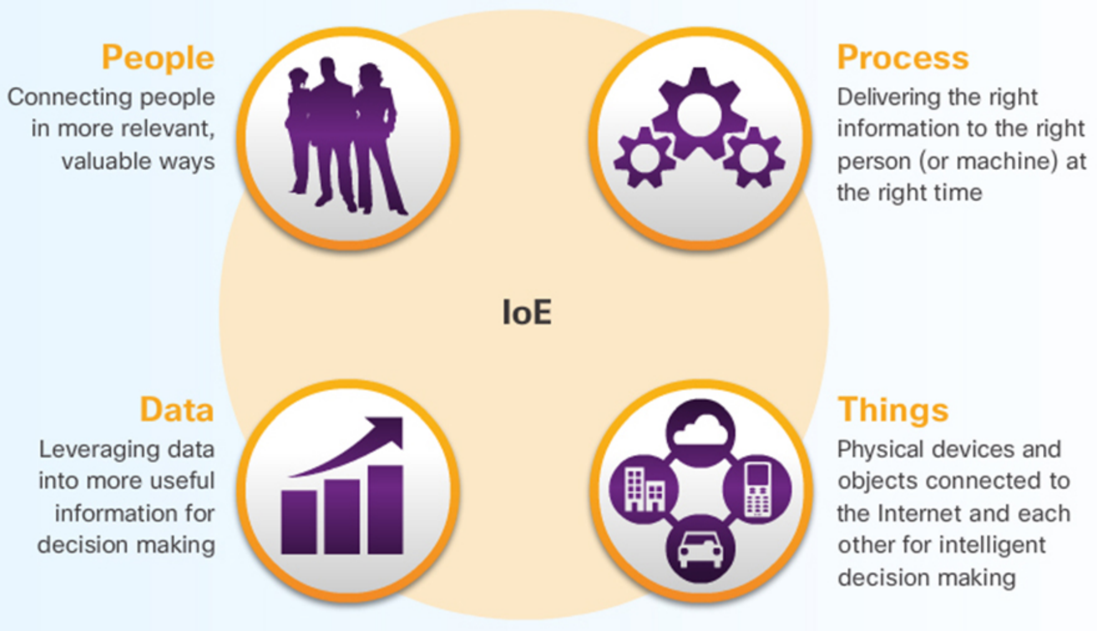

People
Connecting people in more relevant, valuable ways
Process
Delivering the right information to the right person (or machine) at the right time
IoE
Data
Leveraging data into more useful information for decision making
Things
Physical devices and objects connected to the Internet and each other for intelligent decision making

Figure 24 The four pillars

The four pillars of the IoE are People, Process, Data, and Things.

Things

For the IoE to function, all of the devices that are part of the intended IoE solution must be connected together so that they can communicate. There are two ways in which devices can be connected; either wired or wirelessly. Devices that are not traditionally connected to the network require sensors, RFIDs, and controllers.

Data

Big Data refers to the vast amount of data generated every hour by billions of connected devices. Big Data requires new products and techniques to manage, store, and analyse it. Part of the solution to the problem of Big Data is virtualisation and Cloud computing.

Big Data refers to the way in which organisations collect and analyse vast stores of data for insights that can help identify trends, predict behaviour, and empower decision makers.

People

Connected people make behavioural transformations based on their access to information. Simultaneously, their changed behaviour affects the information that is generated. This is known as a feedback loop. Organisations use data generated by connected people to refine and target their marketing strategies.

Process

Processes occur between people, things, and data. Today, the IoE brings them all together by combining M2M, M2P, and P2P connections.

Session 3: Connecting the unconnected

3.1 Introduction to connecting things

Network engineering combines a range of different technologies. With different manufacturers and a multitude of systems old a new, standards are required to ensure that they are all able to communicate and remain secure. This section explores protocol standards and why we need them, what is a client server, how cloud and fog computing supports the IoE.

3.1.1 Imagine the possibilities

The internet of things (IoT) is about connecting the unconnected. It allows for things to be accessible by the internet that historically have not been. With 50 billion devices to be connected by 2020, the globe itself will be 'growing a nervous system' and have the ability to sense and respond to ever increasing amounts of data. The IoE is able to improve quality of life for people everywhere by taking advantage of these connected things and the data produced, and incorporating new processes that enable people to make better decisions and offerings.

The following video was filmed in 2011. Some of its predictions have already come to pass, with others well on their way! It highlights the breadth of things still unconnected and the opportunities available in this next decade.

Video content is not available in this format.

3.1.2 Connecting things for consumers

How does connecting things impact us in our personal life? For example, consider the current structure of the average home network.

The home network is a LAN with devices that connect to the home router. Most likely, the router also has wireless capabilities. In this instance, the LAN provides wireless LAN (WLAN) access. Figure 1 shows a typical home WLAN with a connection to the internet through a local internet service provider (ISP). The collection of devices and connections within the ISP are not visible to the home-based customer but are critical for connectivity to the Internet.

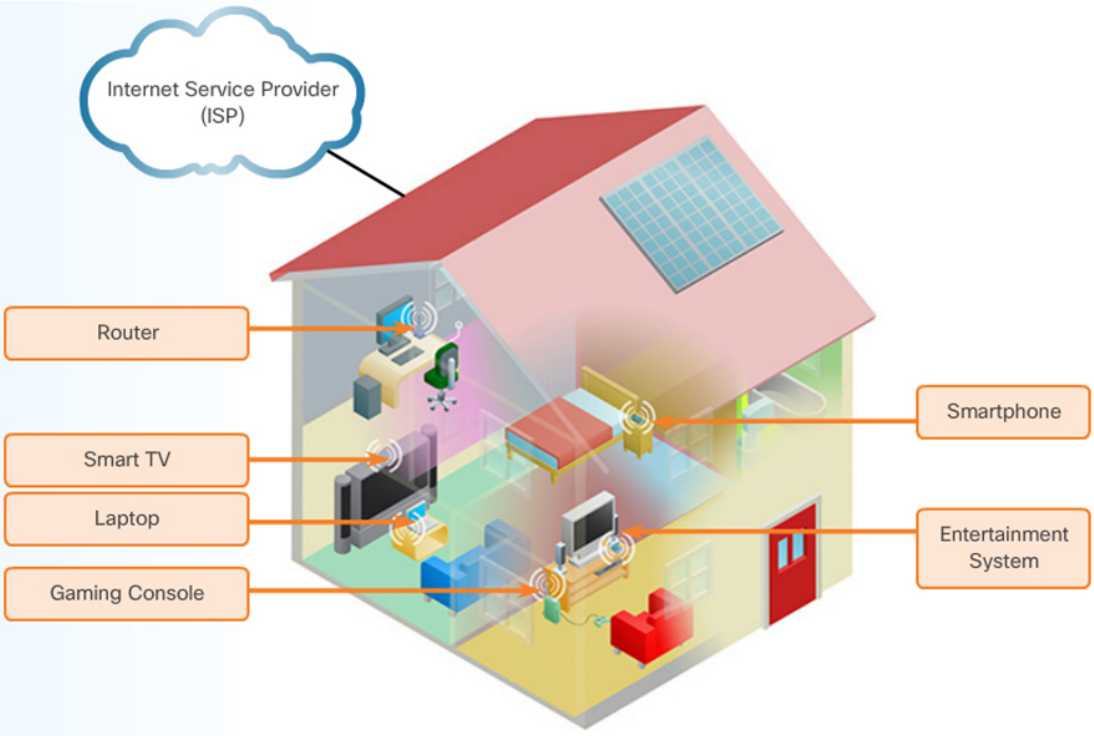


Figure 1

The local ISP connects with other ISPs, allowing access to websites and content around the world. These ISPs connect to each other using various technologies that include WAN technologies, as shown in Figure 2.

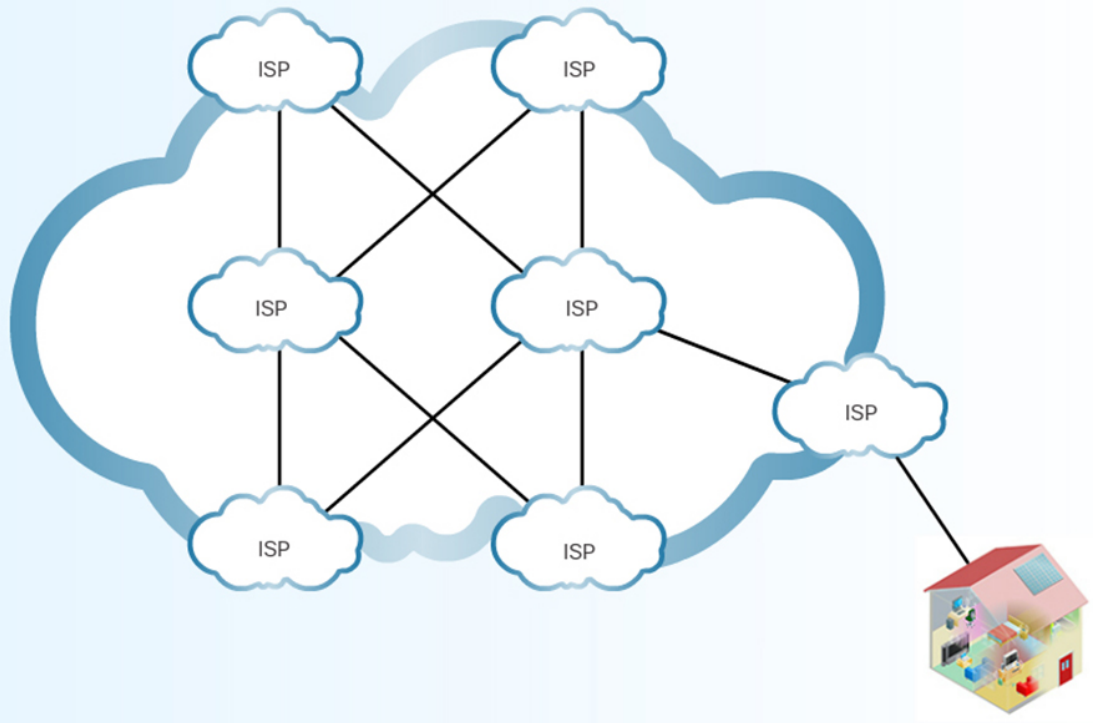


Figure 2

However, the M2M connection is a network type unique to the IoT. Figure 3 depicts a series of fire alarms or home security sensors that can communicate with each other and send data through the gateway router (home router) to a server environment in the Cloud. Here data can be accumulated and analyzed.

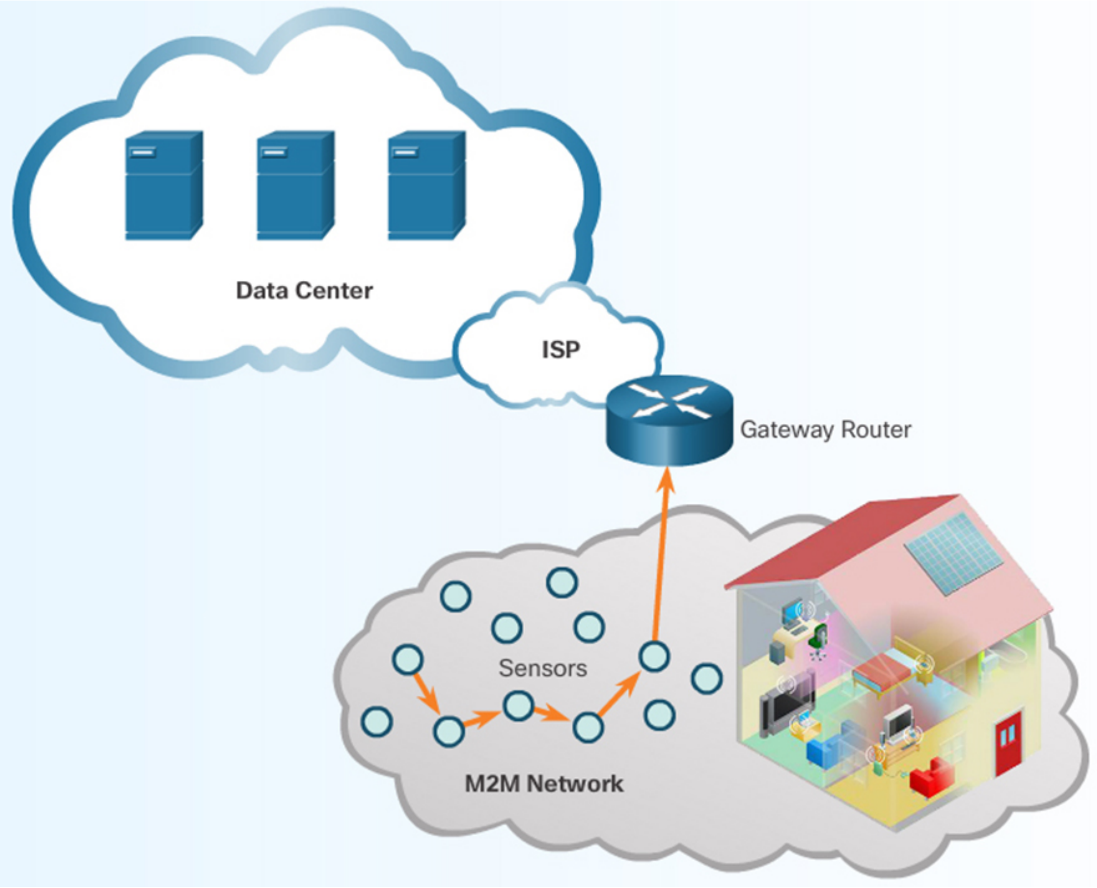


Figure 3

3.1.3 Connecting things for industries

!Warning! CiscoSansTTLight,Helvetica,Arial,sans-serif not supportedIndustrial applications in the IoT require a degree of reliability and autonomy that is not as critical for the consumer environment. Some industrial applications require operations and calculations that happen too quickly to depend on human intervention. For example, if our smartphone fails to remind us of an appointment, it is inconvenient. If the braking system on a large mining truck fails, this can create catastrophic results for the individual and the organisation.

3.1.4 The converged network and things

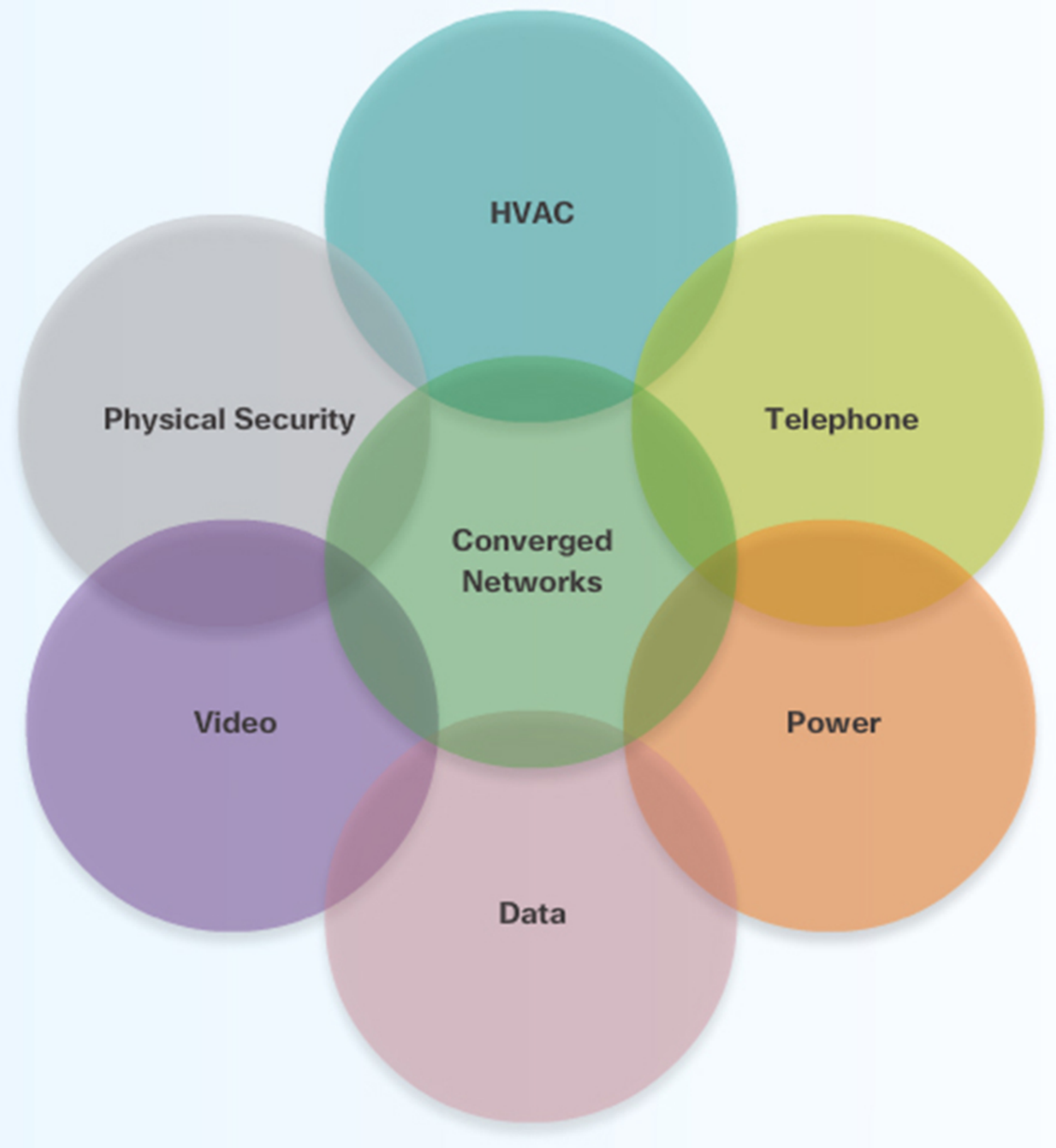


Figure 4 As the IoT evolves, individual networks will be connected together and will include, security, analytics and management

Many things are currently connected using a loose collection of independent, use-specific networks, as shown in the figure. As a result, they cannot be leveraged in the IoE.

For example, today's cars have multiple proprietary networks to control engine function, safety features, and communications systems. Converging these systems onto a common network alone would save over 23 kg (50 lbs) of cable in a modern full-size car.

Other examples include commercial and residential buildings, which have various control systems and networks for heating, ventilation, and air conditioning (HVAC), telephone service, security, and lighting. These disparate networks will converge to share the same infrastructure that includes comprehensive security, analytics, and management capabilities. As the components are connected to a converged network using IoT technologies, they become even more powerful as the full breadth of the IoE is able to take advantage and help people improve their quality of life.

3.1.5 Need for standards

When two devices communicate across a network, they must first agree on a certain set of predetermined rules, or protocols. Protocols refer to the rules of communication that devices use and are specific to the characteristics of the conversation. In our day-to-day personal communication, the rules we use to communicate over one medium, like a telephone call, are not necessarily the same as the protocols for using another medium, such as sending a letter.

Protocols define the details of how messages are transmitted and received. Similar to how people use language to communicate, protocols contain rules for how devices communicate.

A group of inter-related protocols that are necessary to perform a communication function is called a protocol suite. Protocol suites help ensure interoperability between network devices. Individual protocols within a protocol suite may be vendor-specific and proprietary. Proprietary, in this context, means that one company or vendor controls the definition of the protocol and how it functions. Some proprietary protocols can be used by different organisations with permission from the owner. Others can only be implemented on equipment manufactured by the proprietary vendor.

3.1.6 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 set-up 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.

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 see Table 1.

Table 1 Layers of the TCP/IP model

This layer includes many applications that can communicate with the network including web browsers, email programs, and file sharing programs.	TCP operates at this layer managing the conversations between, for example, web servers and web browsers. TCP is also responsible for dividing the data into segments	IP operates at this layer encapsulating each segment into a packet with source and destination addressing information.	Ethernet is one of the primary access methods for transmitting data over a physical link. Standards, such as 802.11, define the

	to be sent down to the Internet layer.		access method for wireless devices.
Application	**Transport**	**Internet**	**Network access**

Objects that are IP-enabled, meaning that necessary TCP/IP software is installed, will have the ability to forward data across the Internet directly.

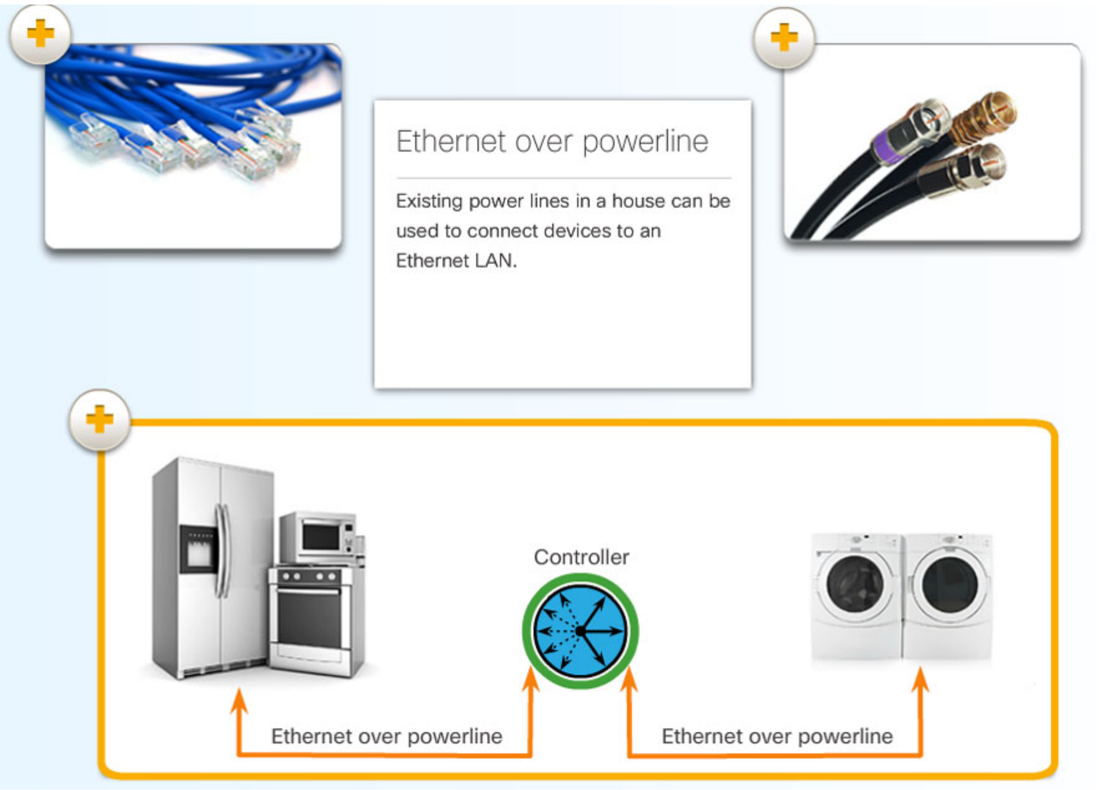
3.1.7 Network connectivity

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 (Table 2 and Figure 5)

Table 2

Category 5 cable (twisted pair)	Coaxial (coax) cable	Ethernet over powerline
Category 5 is the most common wiring used in a LAN. The cable is made up of 4 pairs of wires that are twisted to reduce electrical interference.	Coaxial cable has an inner wire surrounded by a tubular insulating layer, that is then surrounded by a tubular conducting shield. Most coax cables also have an external insulating sheath or jacket.	Existing power lines in a house can be used to connect devices to an Ethernet LAN.



Ethernet over powerline

Existing power lines in a house can be used to connect devices to an Ethernet LAN.

Figure 5 Cables

There are a number of wireless network protocols available today. The characteristics of these protocols vary greatly. Figure 6 provides a few common wireless protocols and shows a visual representation of where these protocols fit in the classification spectrum. Table 3 provides more information about each of the protocols. Notice that a protocol can span multiple classifications.

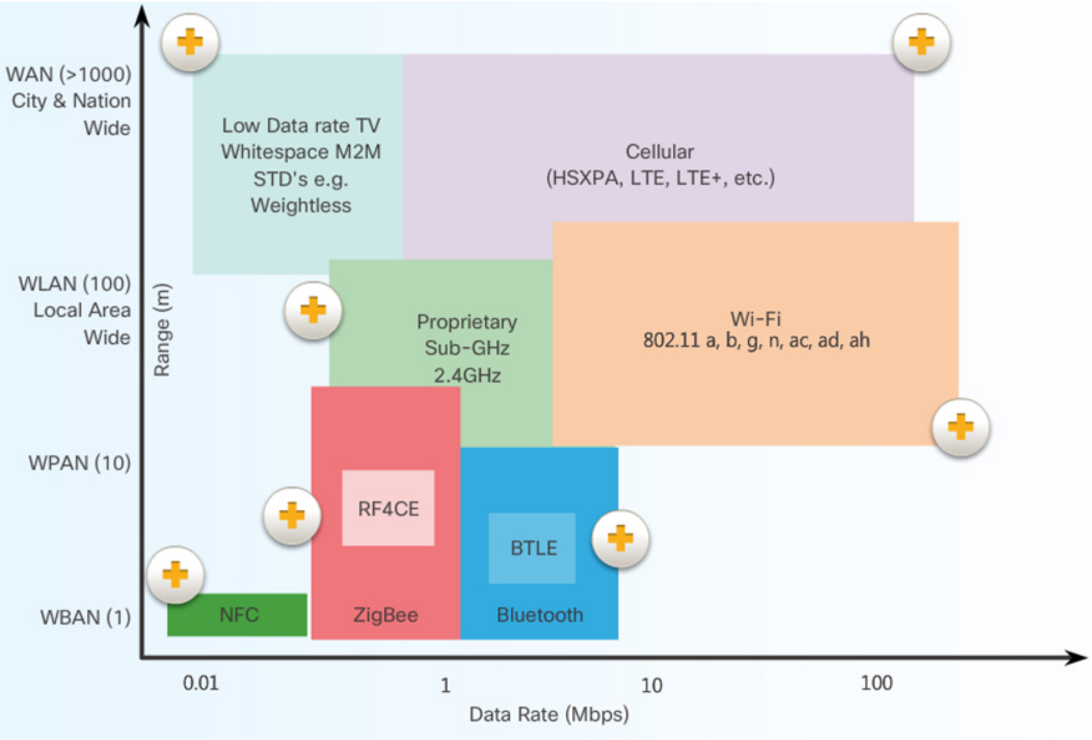


Figure 6

Table 3

Weightless	Cellular	Proprietary	Wi-Fi	NFC	ZigBee	Bluetooth
Uses the unused portions of the spectrum band in and around TV transmissions. It is a low frequency band which enables excellent propagation without needing large antennas in devices. It has relatively low output power.	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.	This is a communications protocol owned by a single organisation or individual.	This is the name of a popular wireless networking technology that uses radio waves to provide wireless high-speed Internet and network connections.	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.	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 Low Energy (BTLE) is being adopted by the health care industry for portable medical and lifestyle devices.

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

3.1.8 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. For example, a device that does not use TCP/IP may still communicate with another device that does using a standard, such as Institute of Electrical and Electronics Engineers (IEEE) 802.15 (Table 4).

Table 4

Bluetooth	ZigBee	NFC	6LoWPAN
The Bluetooth protocol is typically used between devices that are in close range, such as a smartphone connection to a Bluetooth-enabled headset, or a Bluetooth-enabled wireless keyboard connected to a computing device.	ZigBee is 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.	Near field communication (NFC) 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.	6LoWPAN arose from the need to include extremely low-powered devices with limited processing capabilities as part of IoT, for example, smart meters in a small network.

3.1.9 Client–server model

Understanding network connectivity is an important part of understanding how data is moved across the network.

Since the inception of the internet, the primary method that businesses use to process data has been through a client-server model. Consider the way organisations might implement file servers. End users within an organisation can store any number of files and documents on the file server, allowing end devices to conserve memory and processing power for use on local applications. By storing files on a central file server, other users within the organisation can easily access these files, which allows for greater collaboration and sharing of information. Finally, with centralised services (such as file servers), organisations can also implement centralised security and backup procedures to protect those resources.

With the growth of the internet and the expansion of mobile users, the client-server model is not always the most effective option. As more individuals connect from greater distances, having a centralised server may not be optimal. Those that are farther away from the server may experience greater delays and more difficulties accessing the information. These changes in requirements for organisations and individuals have led to cloud computing.

Figure 7 depicts the relationship between email client, web client and file client and their respective servers. Press the plus buttons to reveal the different relationships.

Interactive content is not available in this format.
Figure 7

3.1.10 Cloud computing model

Cloud computing is different from the client–server model in that servers and services are dispersed all over the globe in distributed data centres. With cloud computing, there is a significant shift in workload. Cloud computing allows end users to access applications from servers located in the cloud instead of requiring an end device client.

In Cloud computing, data is synchronised across multiple servers, so that servers in one data centre maintain the same information as servers in another location. Organisations simply subscribe to different services within the cloud. Individual organisations are no longer responsible for maintaining the application updates, security, and backups. This becomes the responsibility of the organisation offering the cloud service.

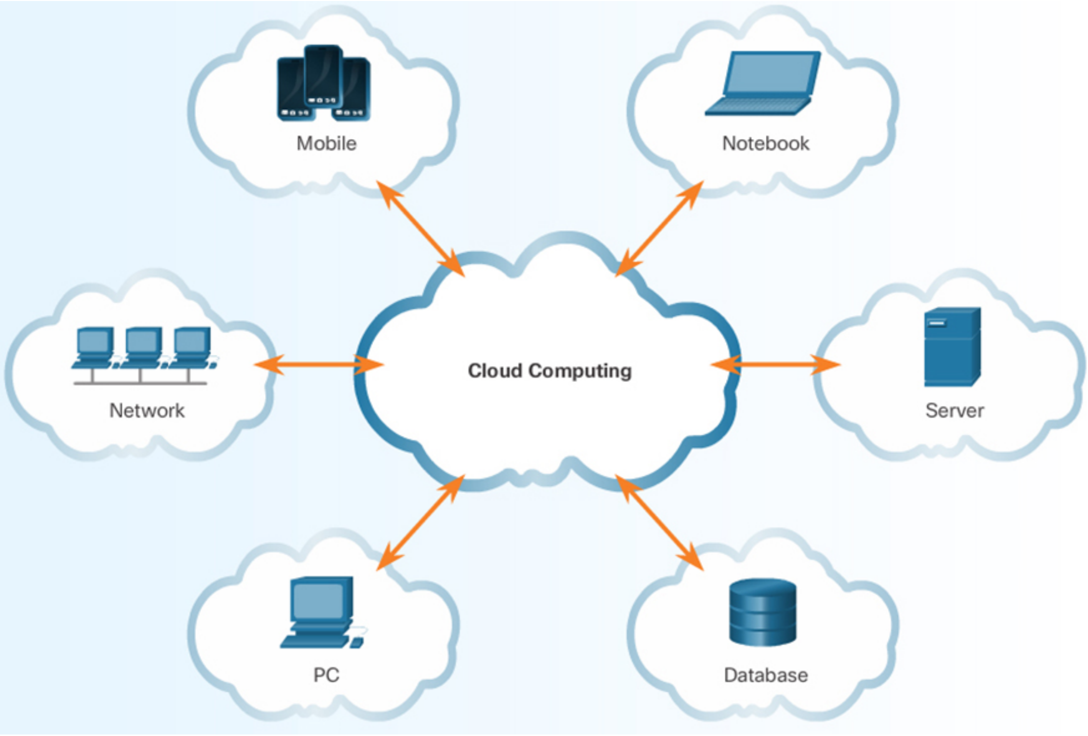


Figure 8

Microsoft Outlook is a client–server system that is typically set up for a specific organisation. End users connect to the email server using a locally installed email client. Gmail is a cloud computing program that allows users from anywhere to log into their Gmail account. A user is able to create, access, and modify emails from virtually anywhere that they have an Internet connection, over a variety of devices and operating systems. Users no longer must keep email clients up-to-date or install new features; these application updates are performed automatically on the server.

3.1.11 Fog computing model

Cloud computing has solved many problems of the traditional client–server model. Cloud computing may not be the best option for delay-sensitive applications that require an immediate, local response.

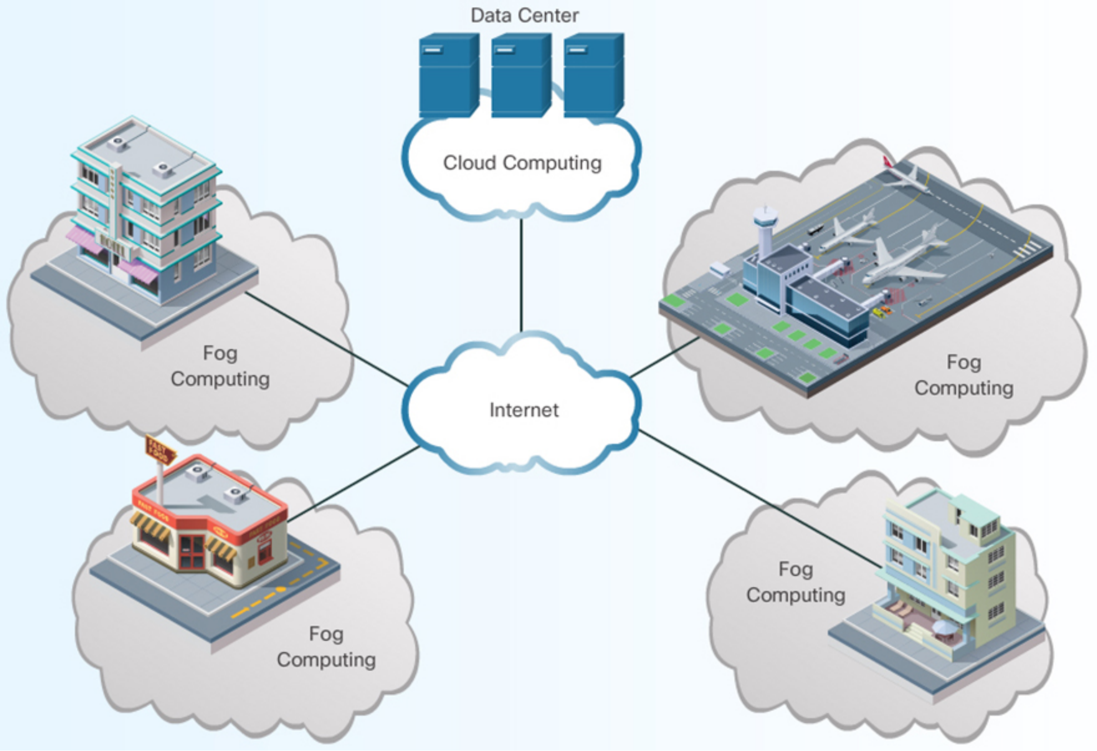


Figure 9

The emerging wave of the IoT requires mobility support and geographical distribution, in addition to location-awareness and minimised delay. Devices in the IoT will require real-time data and quality of service mechanisms. The IoT encompasses an almost limitless number of IP-enabled devices that can monitor or measure nearly anything. However, the one thing these devices have in common is that they are distributed throughout the world.

One of the most significant challenges this presents is creating links between these devices and the data centres where data can be analysed, as shown in the figure. These devices can produce huge amounts of data. For example, in just 30 minutes a jet engine may produce 10 terabytes of data about its performance and condition. It would be inefficient to deliver all the data from IoT devices into the cloud to be analyzed and then forward decisions back to the edge. Instead, some of the analysis work should take place at the edge, for example, on industrial-strength Cisco routers built to work in the field.

Fog computing creates a distributed computing infrastructure closer to the network edge that carries out easier tasks that require a quick response. It reduces the data burden on networks. It enhances resiliency by allowing IoT devices to operate when network connections are lost. It also enhances security by keeping sensitive data from being transported beyond the edge where it is needed.

3.1.12 Smart traffic light system

Consider the smart traffic light system as a good use of fog computing.

A smart traffic light system illustrates support for real-time interactions. The system interacts locally with a number of sensors. The sensors detect the presence of pedestrians and bikers, and measure the distance and speed of approaching vehicles. The system also interacts with neighbouring lights to coordinate with traffic lights. Based on this information, the smart light sends warning signals to approaching vehicles and modifies its own cycle to prevent accidents.

Re-coordinating with neighbouring smart traffic light systems in the fog allows for any modification of the cycle. The data collected by the smart traffic light system is processed locally to do real-time analytics. For example, it changes the timing of the cycles in response to road conditions. The data from clusters of smart traffic light systems is sent to the cloud to analyse long-term traffic patterns.

3.2 Introduction to configuring things

The configuration of different devices is at the heart of many technological disciplines − chances are you have configured the computer/tablet/phone that you are using to read this course. In this section you will explore the different types of technologies in use, this will include: how IP (internet protocol) addresses are allocated, different end devices, sensors, actuators and controllers, which infrastructure devices are used on the internet and your network to support the IoE.

3.2.1 End devices in the IoT

!Warning! CiscoSansTTLight,Helvetica,Arial,sans-serif not supportedAs previously described, end devices connect to the Internet and send data across the network. Cell phones, laptops, PCs, printers, and IP phones are examples of end devices using the Internet protocol (IP). Today there are new types of end devices that collect and transmit data, but use different protocols such as IEEE 802.15 and NFC. These non-IP-enabled devices are critical enablers of the IoT.

3.2.2 Sensors

In the IoT, another type of device, called a sensor, must be connected to the data network. A sensor is an object that can be used to measure a physical property, and convert that information into an electrical or optical signal. Examples of sensors include those that can detect heat, weight, motion, pressure, and moisture.

Sensors are typically purchased with pre-programmed specific instructions; however, some sensors can be configured to change their degree of sensitivity or the frequency of feedback. The sensitivity setting indicates how much the sensor's output changes when the measured quantity changes. For example, a motion sensor can be calibrated to detect the motion of people, but not pets. A controller, which may include a graphical user interface (GUI), is used to change sensor settings, either locally or remotely.

Table 5

Oil, gas, mining	Cities	Transportation	Utilities	Agriculture
Sensors detect chemical levels such as carbon monoxide, carbon dioxide, oxygen, methane, hydrogen, ammonia, and hydrogen sulfide.	Some sensors include pressure (for parking), dust concentrations, noise, displacement of cracks, temperature, humidity, and luminosity.	Sensors measure idle times, fuel usage, engine faults, and engine load.	Sensors measure idle times, fuel usage, engine faults, and engine load.	Sensors detect soil moisture, leaf wetness, solar radiation, atmospheric pressure, and stem diameter.

3.2.3 Actuators

Another device that is implemented within the IoT is an actuator. An actuator is a basic motor that can be used to move or control a mechanism or system, based on a specific set of instructions. Actuators can perform a physical function to 'make things happen'. One type of industrial actuator is an electric solenoid used to control hydraulics .

There are three types of actuators used in the IoT:

- **hydraulic** – uses fluid pressure to perform mechanical movement
- **pneumatic** – uses compressed air at high pressure to enable mechanical operation
- **electrical** – powered by a motor that converts electrical energy to mechanical operation.

Regardless of how the actuator causes the movement to be performed, the basic function of an actuator is to receive a signal, and based on that signal, perform a set action. Actuators are typically not able to process data. Rather, the result of the action performed by the actuator is based on a signal received. The action performed by the actuator is typically caused by a signal from the controller.

3.2.4 Controllers in the fog

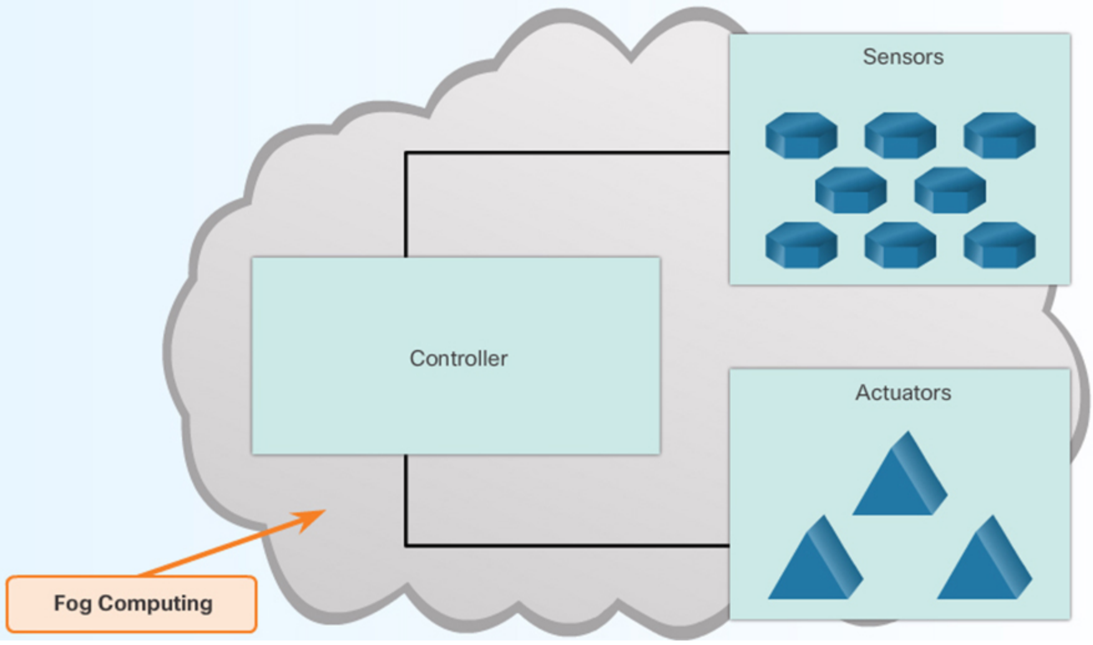


Figure 10

Sensors collect data and forward that information to the controllers. The controller can forward any information gathered from the sensors to other devices in the Fog, as shown in the figure.

Recall the example of a smart traffic light system. The sensors detect and report activity to the controller. The controller is able to process this data locally and determine optimal traffic patterns. Using this information the controller will send signals to actuators in the traffic lights to adjust traffic flows.

This is an example of M2M communication. In this scenario, the sensors, actuators, and the controller all exist within the Fog. That is, information is not forwarded beyond the local network of end devices.

Processing data in the fog is occurring in less traditional networking environments. New places in networking, or PINs, are created as more things in various industries connect to the network. Field Area Networks (FANs) place hardened equipment in harsh or exposed environments. Smart Grid is an example of a FAN. More detailed information is available from the Cisco website Field Area Network.

3.2.5 IP-enabled controllers

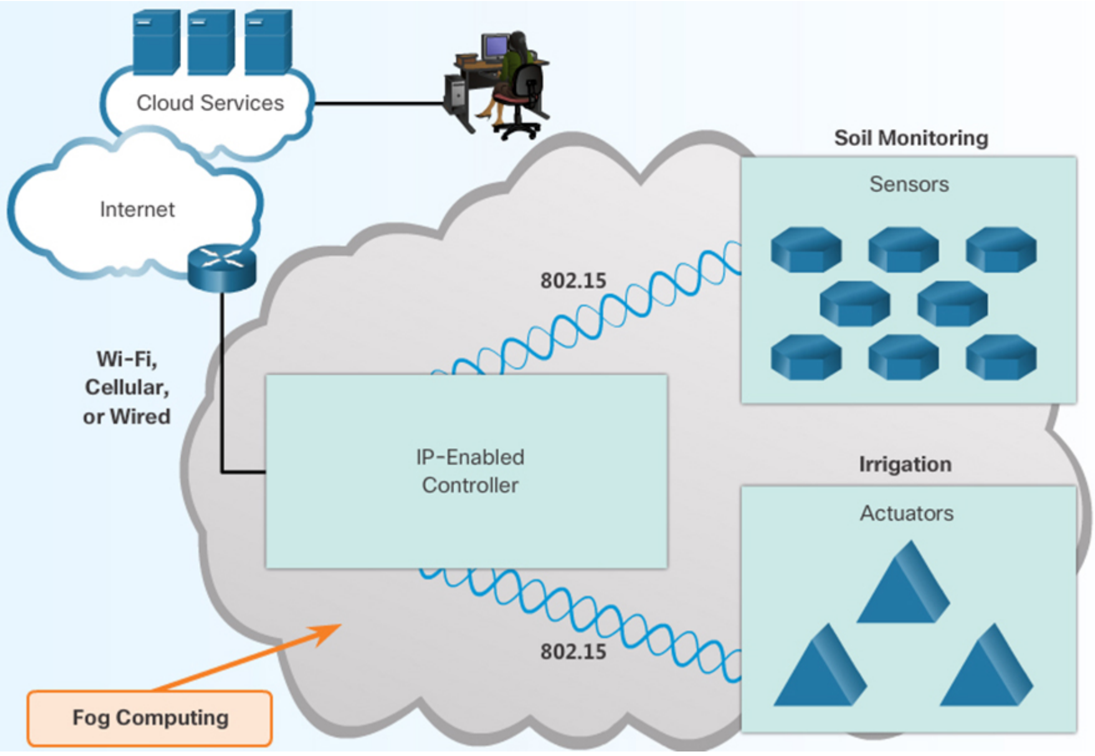


Figure 11

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

Consider the scenario of a coffee plantation, as shown in the figure. The plantation owner wants to monitor the plants to determine the best time to harvest beans. Sensors can be used to collect information on the physical aspects of the plants, such as weather, soil conditions, and carbon dioxide levels. This information is forwarded to the controller. The controller forwards a more complete picture of the information to a network server or across the Internet to a Cloud-based service. Information gathered by the sensor nodes and controller can be further analyzed and accessible via mobile and remote devices.

In this scenario, the controller collects information from the sensors using the 802.15 protocol ZigBee. The controller consolidates the information received, and forwards the data to the gateway using the TCP/IP protocol suite.

Controllers, sensors, and actuators will contribute greatly to the expansion of things that get connected in the IoT.

3.2.6 IP-enabled sensors

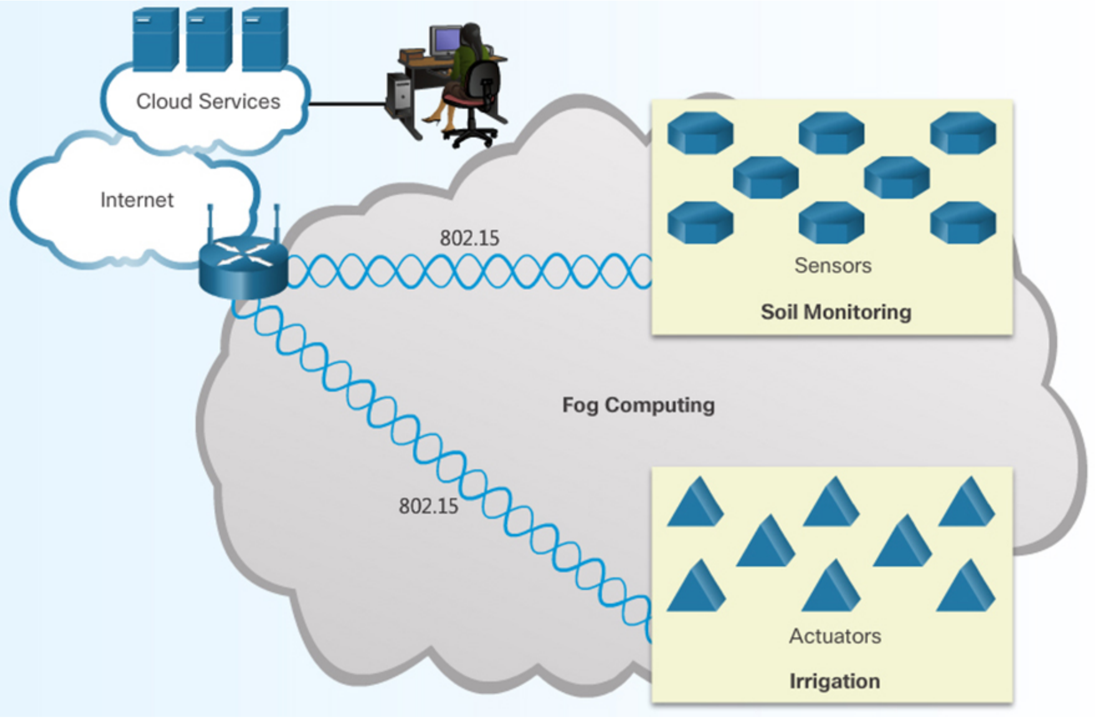
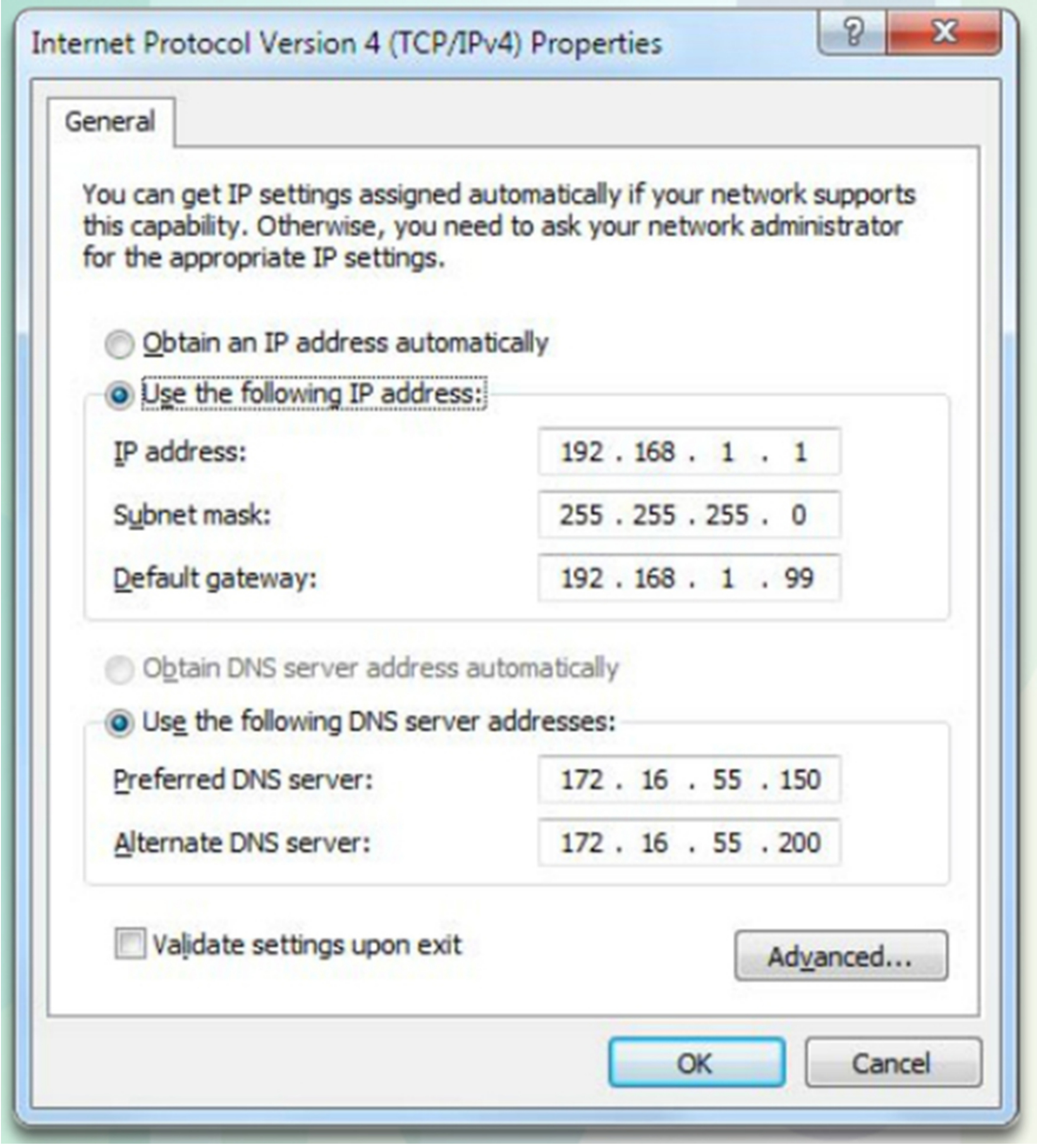


Figure 12

Some sensors and actuators support TCP/IP, which removes the need for a controller.

The figure shows sensors and actuators connected directly to the cloud, through a gateway. In this example, the gateway performs the routing function necessary to give IP-enabled devices Internet connectivity. The data these devices generate can be transported to a regional or global server for analysis and further processing.

3.2.7 Static IP addressing



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address:	192 . 168 . 1 . 1
Subnet mask:	255 . 255 . 255 . 0
Default gateway:	192 . 168 . 1 . 99

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server:	172 . 16 . 55 . 150
Alternate DNS server:	172 . 16 . 55 . 200

□ Validate settings upon exit

Figure 13

For any IP-enabled device to communicate over an IP network, it must be configured with the correct IP address information. Typically, this information is configured within the device settings. You can statically, or manually, configure IP addressing, as shown in the figure for a Windows PC.

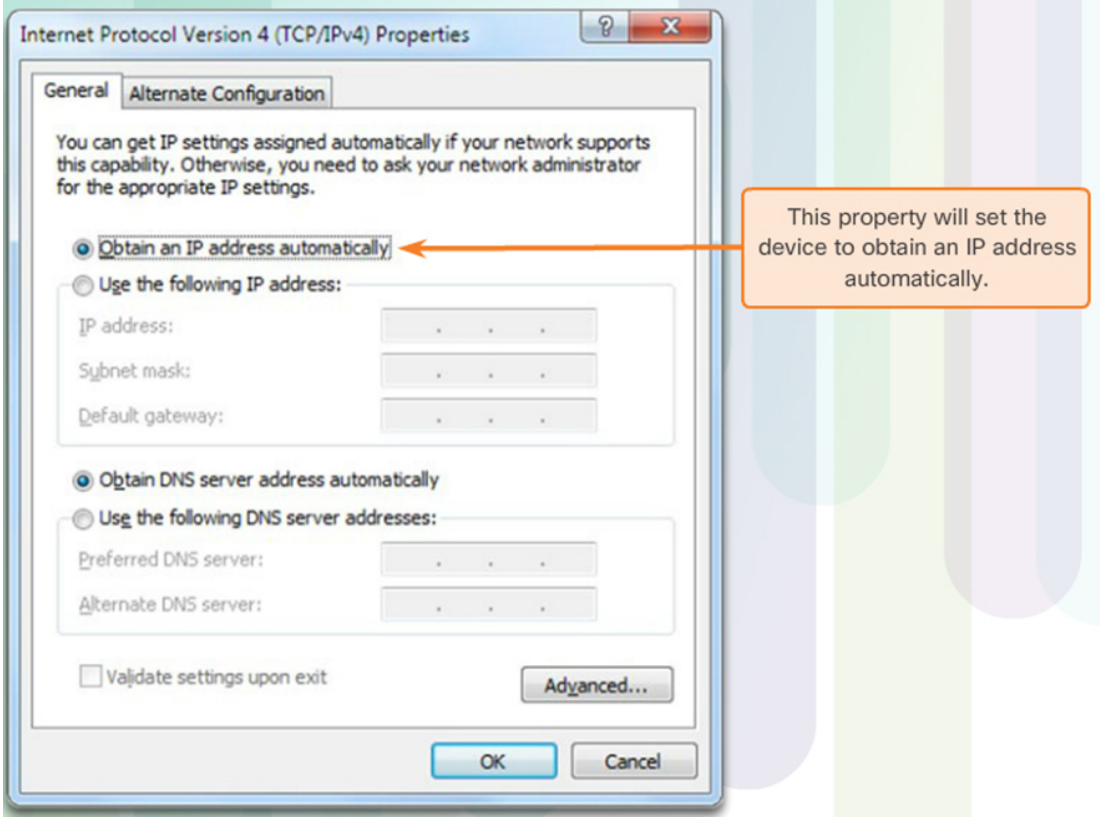
As we learned earlier, an IP address is similar to a street address in that it identifies a unique location across the globe. Your local postal office is your 'gateway' to the postal service, which will use its network of postal locations and transport mechanisms to deliver your letter to the proper destination address. In a network, your local postal office is called the "default gateway" with its own IP address. The default gateway is an IP address that is often assigned by the network administrator or the ISP.

Traditionally, devices on the Internet used IPv4 addresses. However, with an increasing Internet population and a limited number of IPv4 addresses, the transition to IPv6 (another enabler of the IoE) has begun. IPv6 has a larger 128-bit address space, providing for 340 undecillion addresses. 340 undecillion is written as the number 340, followed by 36 zeroes! IPv4 only has a theoretical maximum of 4.3 billion addresses, and those are nearly used up.

The IP addresses in the figure are IPv4 addresses. This is an example of an IPv6 address:

2001:0DB8:0000:1111:0000:0000:0000:0200

3.2.8 Automatic IP addressing



Internet Protocol Version 4 (TCP/IPv4) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address:

Subnet mask:

Default gateway:

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server:

Alternate DNS server:

□ Validate settings upon exit

This property will set the device to obtain an IP address automatically.

Figure 14

If you have never entered an IP address on any of your personal devices, it is because the IP address information is automatically assigned to any end device by the Dynamic Host Configuration Protocol for IPv4 (DHCP).

Imagine the amount of time it would take if every end device connected to the network required IP addressing information to be entered manually. Multiply that by every user, every mobile device, and every IP-enabled device on the network, and it becomes overwhelming. With DHCP, end users walk into areas served by a given network, plug in an Ethernet cable or enable a wireless connection, and they are immediately allocated the IP address information.

As shown in the figure, to configure DHCP on a Windows PC, the **Obtain an IP address automatically** option is selected. Your device is assigned information from an IP address pool and associated IP information set up on the DHCP server.

When deploying IPv6, there are other methods that allow a device to obtain its IPv6 addressing information. Stateless Address Autoconfiguration (SLAAC) is a method that allows a device to obtain information from an IPv6 router. Dynamic Host Configuration Protocol for IPv6 (DHCPv6) is similar to DHCP for IPv4, allowing a device to receive information from a DHCPv6 server.

3.2.9 Role of IoT infastructure devices

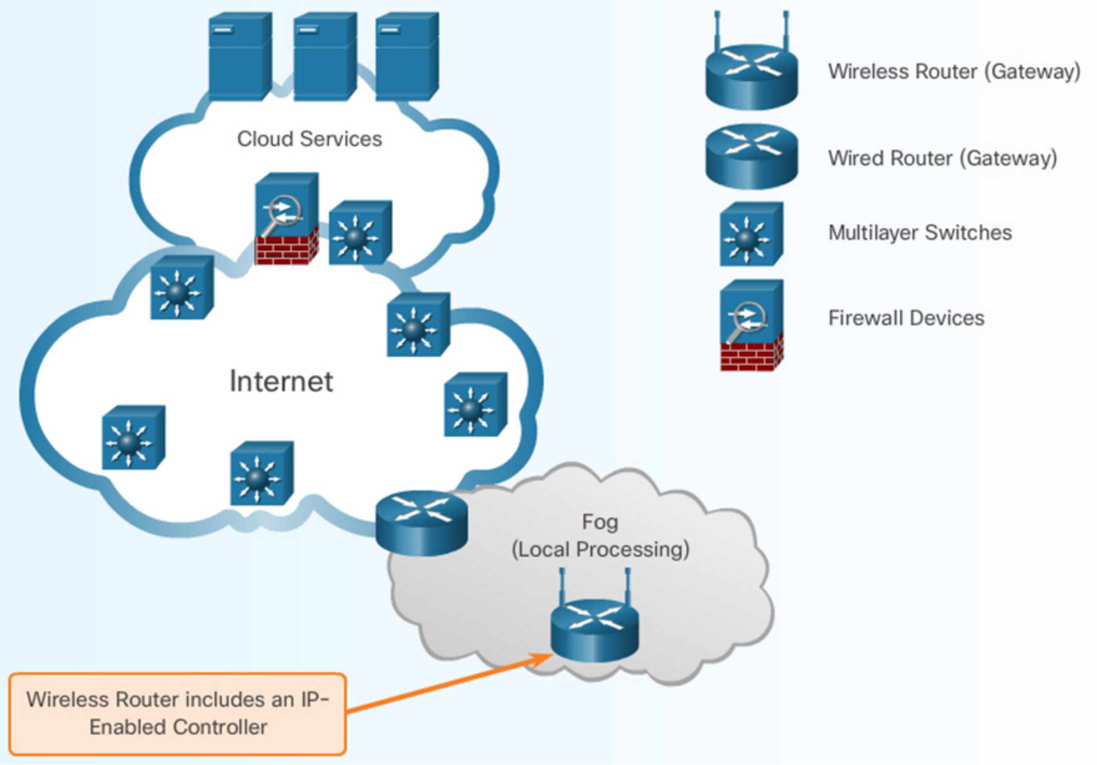


Figure 15

Infrastructure devices are primarily responsible for moving data between the controller devices and other end devices, as shown in the figure.

Infrastructure devices provide a variety of services including:

- wireless and wired connectivity
- quality of service queuing (for example, voice data before video data)
- high availability
- secure transfer.

Infrastructure devices connect the individual end devices to the network, and can connect multiple individual networks to form an internetwork. The management of data as it flows through the network is a primary role of the infrastructure, or intermediary, devices. These devices use the destination end device address, in conjunction with information about the network interconnections, to determine the path that messages should take through the network.

3.2.10 Types of routers

When a source device sends a packet to a remote destination device, the help of routers and routing is needed. A router is a device that routes traffic from the local network to devices on remote networks. A router is required because end devices do not maintain information on where to forward packets to reach remote destinations. A router is an intelligent device that collects information about the location of different networks. The router uses this information to determine the best path to reach those destinations, which is known as the routing process.

There are many types of infrastructure routers available.

Regardless of their function, sise, or complexity, all router models are essentially computers. Just like computers, tablets, and smart devices, routers also require the following:

- operating systems (OS)
- central processing units (CPU)
- input/output (I/O) interfaces
- memory.

Table 6 Examples of Cisco routers

Cisco 819 ISR	Cisco 500 Series Wireless WPAN Industrial Routers	Cisco CRS Multichassis System	Cisco 2000 Series Connected Grid
The Cisco 819 ISR (Integrated Services Router) gateway provides a rapidly deployable, highly available, reliable, and secure solution designed specifically for M2M applications.	Cisco 500 Series Wireless Personal Area Network (WPAN) Industrial Routers (IR500) provide unlicensed 915 MHz industrial, scientific, and medical (ISM) band WPAN communications. They help to enable a diverse set of Internet of Things (IoT) applications. These include smart metering, smart grid, distribution automation, supervisory control and data acquisition (SCADA), and street lighting.	The Cisco CRS (Career Routing System) Multichassis System is the most widely deployed multichassis router, with over 1000 systems operating at many of the world's largest network operators.	The Cisco 2000 Series Connected Grid Router is designed specifically for the harsh, rugged environments often found in the energy and utility industries.

The operating system used in Cisco devices is known as the Internetwork Operating System (IOS). Complete information on Cisco routers is available at the web page Routers.

3.2.11 Cisco ISR 819

To provide M2M connectivity within the IoT, it is often necessary for a router to combine multiple technologies to communicate with multiple devices. The Cisco 819 ISR can combine Wi-Fi with GPS and 3G/4G WAN connectivity and location services. Combining these technologies allows the 819 ISR to function in many different environments. For example, in a transportation environment, mobile network end devices must communicate across long distances using 3G/4G networks. However, in a retail or manufacturing environment, Wi-Fi may be the best network option for stationary devices.

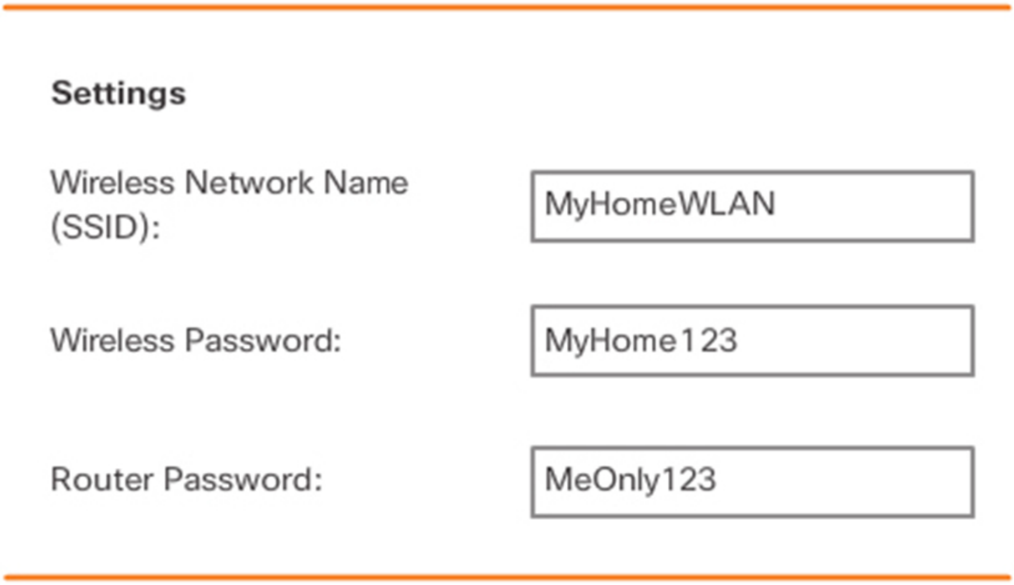
Computing capability can be built into Cisco IoT routers and switches. Cisco combines Linux with IOS, to create a distributed computing infrastructure to equip routers for Fog computing. This architecture is called IOx. IOx makes it easier to connect specialised, industry-specific systems at the edge of the network to create new sensing and control functions with Cisco routers.

The Cisco ISR 819 is part of a family of devices, the Cisco website has a section on the 810, which includes the 819.

3.2.12 Small business and home routers

!Warning! CiscoSansTTLight,Helvetica,Arial,sans-serif not supportedIn addition to the more dedicated enterprise devices, like the Cisco IOS 819 ISR, there are also low-cost multifunction devices available for home and small business networks. These wireless routing devices offer integrated routing, switching, wireless, and security capabilities. Modern wireless routers offer a variety of features and most are designed to be functional right out of the box, using the default settings. However, it is good practice to change the initial, default configurations.

3.2.13 Types of ports



Settings

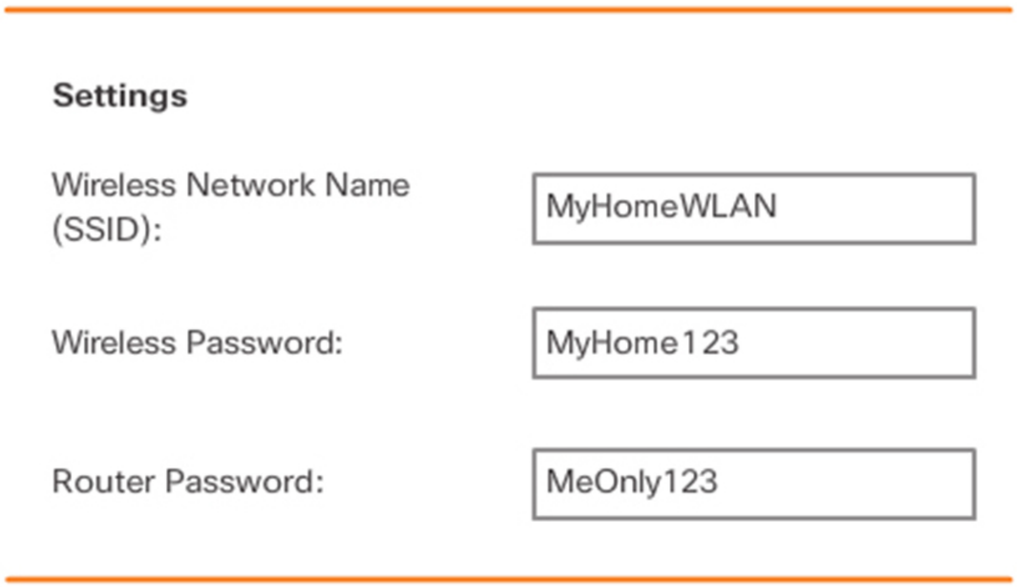
Wireless Network Name (SSID):	MyHomeWLAN
Wireless Password:	MyHome123
Router Password:	MeOnly123

Figure 16

Small business and home routers typically have two primary ports:

- **Ethernet ports** – These ports connect to the internal switch portion of the router. These ports are usually labelled 'Ethernet' or 'LAN'. All devices connected to the switch ports are on the same local network.
- **Internet port** – This port is used to connect the device to another network. The Internet port connects the router to a different network than the Ethernet ports. This port is often used to connect to the Internet.

3.2.14 Settings



Settings

Wireless Network Name (SSID):	MyHomeWLAN
Wireless Password:	MyHome123
Router Password:	MeOnly123

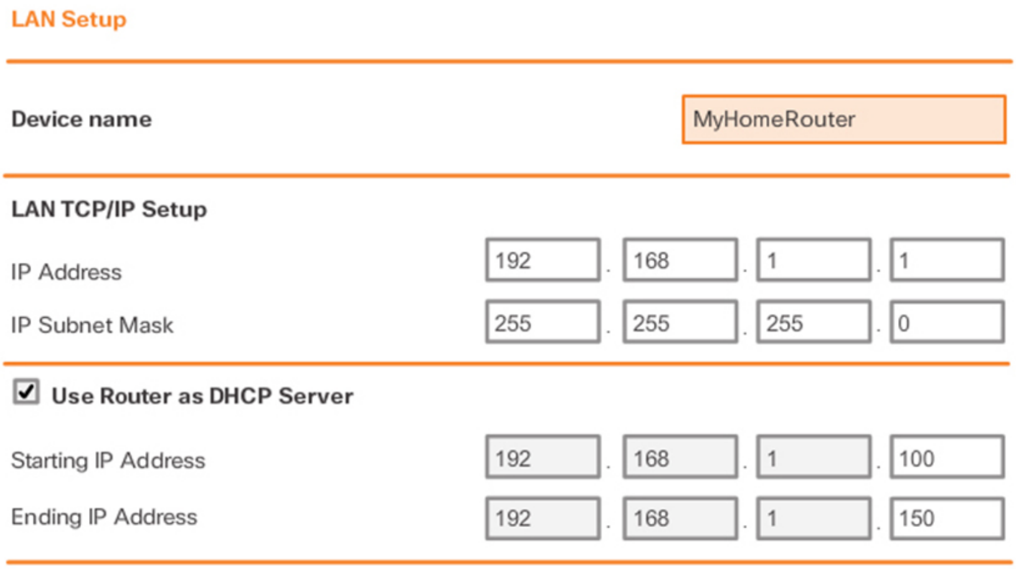
Figure 17

Most of these small wireless routers are configured using a GUI web interface, as shown in the figure. Settings that can be configured include:

- **Wireless network name (SSID) –** Name of the WLAN network, if wireless networking is enabled. SSID stands for Service Set Identifier, which is another name for the wireless network. The SSID is, by default, broadcast to wireless clients.
- **Wireless password –** If wireless networking is enabled, this is the password clients use to connect to the wireless network.
- **Router password** –This is the password used to manage the router and, if configured, is required to access the wireless router to make configuration changes.

For most home and small business networks, the wireless router provides DHCP services to local network clients. Clients that wirelessly connect to the wireless router are given the appropriate IP addressing information for communication to occur.

3.2.15 Gateway



LAN Setup

Device name	MyHomeRouter

LAN TCP/IP Setup

IP Address	192	168	1	1
IP Subnet Mask	255	255	255	0

☑ Use Router as DHCP Server

Starting IP Address	192	168	1	100
Ending IP Address	192	168	1	150

Figure 18

When IP-enabled end devices send a packet to a device on a different IP network, the devices must first forward the packet to the default gateway. Typically, the router connected to the local network segment is referred to as the default gateway. In a small business environment the default gateway is the router used to connect the LAN to the Internet.

In many wireless routers, the IPv4 address of 192.168.1.1 is the default for the router, as shown in the figure. This address is the default gateway address for all end devices on the local network (LAN). Wireless and wired clients that connect to the wireless router receive, via DHCP, the default gateway information and an IP address that is within the same network as the default gateway address. Local clients can then forward packets to the wireless router for routing out on to the Internet.

3.2.16 Packet tracer – home IoE implementation

Watch a demonstration of the Packet Tracer – Home IoE Implementation activity.

Video content is not available in this format.

Cisco | Networking Academy®
Mind Wide Open™
Packet Tracer - Home IoE Implementation
cisco

The video demonstration is the primary source for how to navigate the activity. However, after viewing the video, you can use the following files to investigate the activity on your own.

- Packet Tracer – Home IoE Implementation.pdf
- Packet Tracer – Home IoE Implementation.pkz

Essential note: If you are new to Packet Tracer, you can watch a tutorial. You must install Packet Tracer before you can open .pkz files. To install Packet Tracer, return to the course progress page where a copy is available to download and install .

Packet Tracer is available for both Microsoft Windows and Linux systems. The Open University Cisco Academy team support a moderated Facebook Community helping Mac users port this application onto all versions of the Apple Mac OSX. For more information, you will need to join the community.

3.3 Programming

Programming is at the heart of all computing technologies, programmers created the operating system and browser or reader you are using to read this course. By the end of this section you will be introduced to some basic principles and practices in programming.

3.3.1 Programming

As discussed in the previous section, sensors and actuators are used abundantly in the IoT. Sensors measure a physical property and forward that information across the network. How do the sensors know what information to capture or which controller to communicate with?

Actuators perform actions based on a received signal. How does the actuator know which action to perform or which signals are required to activate that action?

Sensors must be told what to capture and where to send that data. A controller must be programmed with a set of instructions to receive that data and decide if it should process and relay that data to another device. For example, IoT end devices, such as the computer installed in a car, must be programmed to react to different road conditions. All of the devices in the IoT must be programmed, thus programming skills are critical to the success of the IoT and the IoE.

3.3.2 Define basic programming

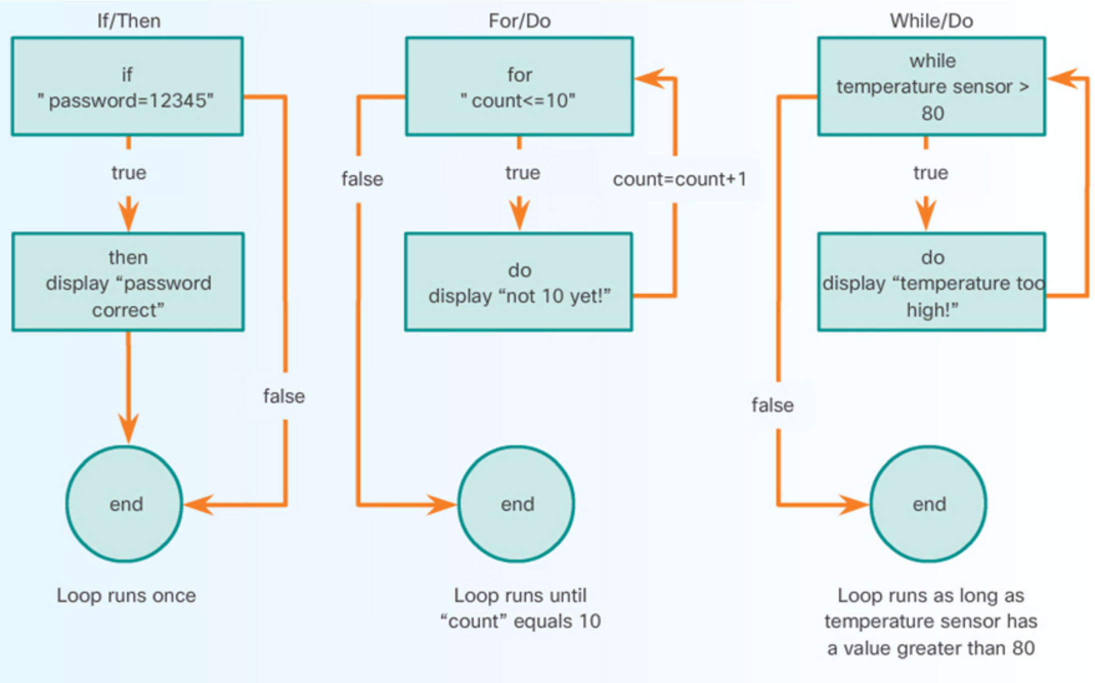


Figure 19

What is a program?

A computer program is a set of instructions given to a computer, to be executed in a specific order. Because computers do not speak human languages, computer programming languages were created. These languages allow humans to write instructions in a way that computers can understand. While there are several different computer languages, all computer languages are based on logical structures.

The figure shows the most common logical structures found in programming languages:

- **IF *condition* THEN *instructions* (If/Then) -** This is one of the most common programming structures. It is used to introduce conditional code execution. The set of instructions following the THEN keyword is only executed if the *condition* given is true. If the *condition* is false, the *instructions* are never executed. For example, IF *password* = *12345*, THEN display*'password correct'.* The code above would only show the 'password correct' message if a password of 12345 is entered.
- **FOR *expression* DO *instructions* (For/Do) -** This logical structure is used to create controlled loops. The set of instructions is executed as many times as defined in*expression*. When *expression* is no longer met, the loop ends and the computer moves on to the next instruction. For example, FOR *count*<=*10* DO display *'not 10 yet!'*. The program will check the value of the variable called count. As long as the count is less than or equal to 10, it will display 'not 10 yet!' on the screen. As soon as the count is greater than 10, the structure is abandoned and the computer moves on to the next line of code.
- **WHILE *condition* DO *instructions* (While/Do) -** The WHILE logical structure is also used to create controlled loops, but in a different way. WHILE executes *instructions* as long as the*condition* is true. When the *condition* is no longer true, the structure is abandoned and the computer moves on to the next line of code. For example, WHILE temperature sensor> 80DO*show 'temperature too high!'* on screen*.* The message 'temperature too high!' will display repeatedly until the value of the temperature sensor is less than or equal to 80.

Logical conditions like these are the building blocks of computer programs.

3.3.3 Types of programs

Different programs perform different tasks. For example, there are programs to measure and report temperature, programs governing traffic lights, and programs that allow us to interact with computers and devices.

Sometimes a program category is so common that it receives its own name. A few categories include:

- **Firmware −** Firmware contains the instructions that the device performs as it boots up. This might be the only software on the device or it may contain instructions to load a more robust operating system. Examples of devices that use firmware include watches, printers, TV sets, sensors, cell phones, routers, and switches. Firmware usually has a considerably smaller set of functionalities and is therefore much smaller in size.
- **Operating systems −** These are programs written to allow humans to interact with a computer. Examples of operating systems are Windows, Mac OS, Linux, Apple iOS, Android, and Cisco IOS, as shown in the figure.

- **Applications −** These are programs designed and written to perform a specific task or service. Word processors, image editing tools, spreadsheet editors, collaboration tools, data analysis and monitoring tools are all considered applications.

3.3.4 Programming languages

There are many different computer languages used to write computer programs, for example C++ and Java. For example, the C language is a popular computer programming language. Entire operating systems were written in C. It was initially developed between 1969 and 1973, however, its evolution into the object-oriented C++ and later to C# kept this language relevant.

Java (not be confused with JavaScript) is another popular object-oriented programming language. Released by Sun in 1995, Java focuses on multiple platforms designed to require as few implementation dependencies as possible. The WORA (write once, run anywhere) acronym is often identified as a characteristic of Java. Due mostly to its multiplatform aspect, Java is widely used on the web.

3.3.5 JavaScript programming example

To give you a better understanding of computer programs, it is useful to analyse some JavaScript code.

JavaScript is a scripting language used primarily in web applications. For example, consider a fictional web application called Cisco Coffee. This application is designed to act as a monitoring tool, or dashboard, for a coffee farm. Figure 18 shows a coffee farm.

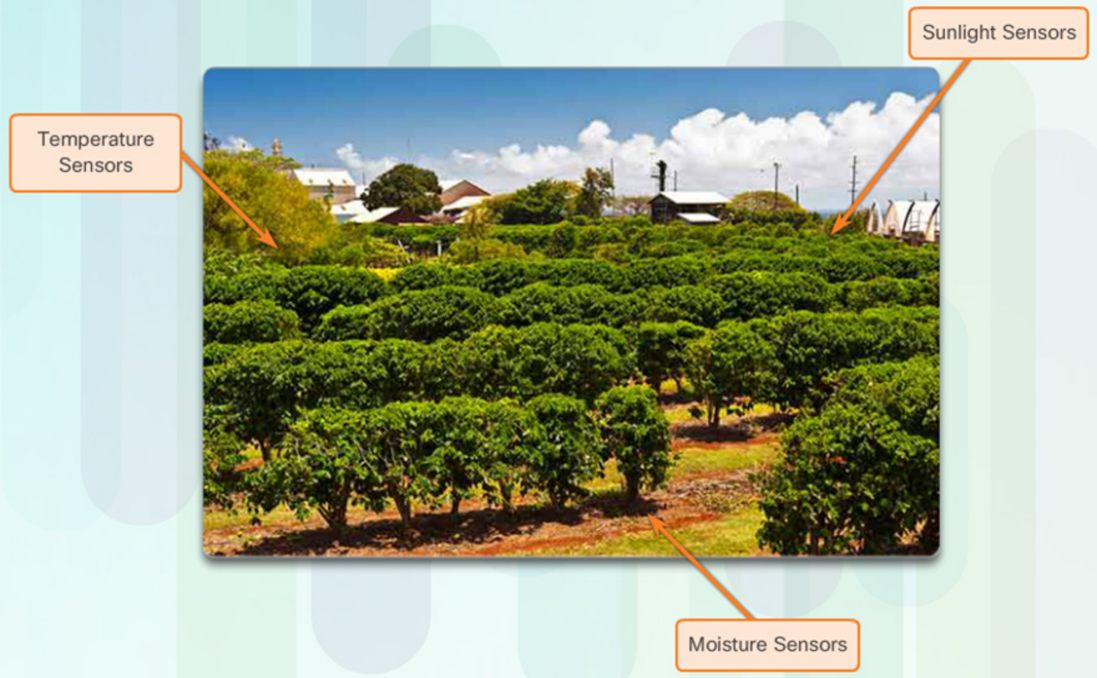


Figure 20

In this scenario, many sensors are installed in various locations in the coffee field, close to the coffee bean plants. These sensors report data back to a central station. This station uses the Cisco Coffee web interface to allow users to monitor the field.

Three types of sensors are installed: temperature, sunlight, and soil moisture. If the temperature drops below 77°F, a warning is presented on the interface screen. If the coffee plants are exposed to too much sunlight, a different warning is presented. If the soil becomes too wet or too dry, a different warning is shown.

The following JavaScript snippets are used to implement these tests.

```
if (temp < 77) {
document.getElementById("logArea").innerHTML =
"WARNING: Field temperature dropped below 77F.";
}
```

If the temperature drops below 77 degrees, then trigger an alert.

```
if (sun > 17000) {
document.getElementById("logArea").innerHTML =
"WARNING: There's too much sunlight on the coffee plants.";
}
```

If the sunlight is greater than 17000 lux, then trigger an alert.

```
if (if ((moist &lt; 5) || (moist > 20)) {
document.getElementById("logArea").innerHTML =
"WARNING: Field moisture level is out of the optimal range."
}
```

If the moisture is less than 5 or greater than 20, then trigger an alert.

Warnings provide an opportunity for feedback loops. For example, if the soil moisture level is low, it might be necessary to activate the irrigation system and alert the farmer who may be aware of other circumstances and can make an appropriate decision. The farmer might decide to intervene and turn off the irrigation system because rain is in the forecast. Regardless of how the irrigation occurs, the sensor reporting soil moisture should begin showing more desirable levels, completing the feedback loop.

3.3.6 The Cisco Coffee JavaScript application

Interactive content is not available in this format.

Figure 21

The figure shows a simulated version of the Cisco Coffee JavaScript application currently running in your browser. If you click **Show Real Data**, you will see a status message that says, 'No sensors found'. That is because there are no actual sensors attached to the application. The application is generating fictitious sensor data. While the entirety of the code is out of the scope of this course, feel free to open the file and analyse it on your own to see how much you understand.

You can view the source by right-clicking anywhere in the figure and choosing an option similar to **View Source** or **View Frame Source,**depending on the browser. Scroll down to the section in the code that starts with **Script**. Lines that began with a double forward slash (//) denote comments. The comments provide a brief explanation of the code. If you would like to investigate this JavaScript application further, you can download the following files:

- Lab – Cisco Coffee JavaScript Application (Optional).pdf
- Cisco Coffee JavaScript Files.zip

3.3.7 Learn about Scratch

Scratch is a programming language developed by the Lifelong Kindergarten Group at the MIT Media Lab. It has an active online community to help you create your own interactive stories, games, and animations.

You can learn more about Scratch or try it yourself. There are a number of video tutorials available on the website to help you get started. Scratch 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.

3.4 Terms and concepts practice

This activity will help you to test some of the terms and concepts you've been introduced to.

actuator

Bluetooth

Cloud computing

sensor

controller

Java

TCP/IP

small business or home business wireless router

Linux

6LoWPAN

Match each of the items above to an item below.

a motor that can be used to move or control a mechanism or system according to a specific set of instructions

a short-range wireless communication protocol suite that transmits data via low-powered radio waves

... servers and services are dispersed all over the globe in distributed database centres

a 'thing' that measures a physical property and converts that data into an electrical signal

... forwards data gathered from sensors to other devices on an M2M network

a popular object-oriented programming language that works on multiple platforms

... required for devices that communicate directly across the Internet

connects devices on a local LAN with the internet

an operating system that allows humans to interact with computers

IPv6-based low power wireless communication protocol

3.5 Session 3 quiz

Check what you have learned in Session 3.

Session 3 quiz

Use 'ctrl' (cmd on a Mac) or right-click to open the quiz in a new window or tab then come back here when you're finished.

3.6 Summary

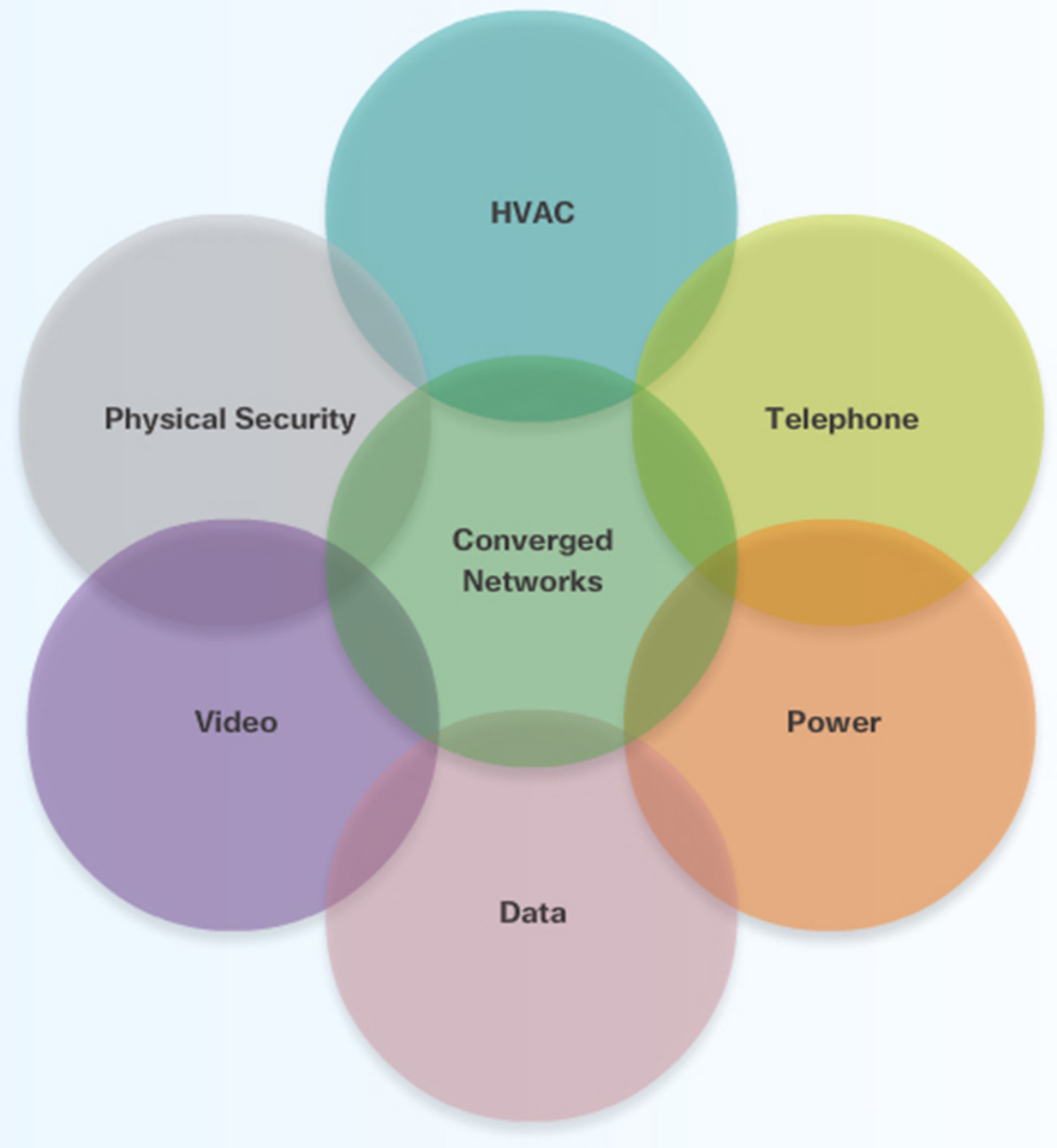


Figure 22

The IoT is made up of a loose collection of disparate, use-specific networks. The M2M connection is a network type that is unique to the IoT.

Protocols refer to the rules of communication that devices use and are specific to the characteristics of the conversation. A group of inter-related protocols is called a protocol suite, which helps ensure interoperability between network devices.

Cloud computing is a type of client-server model in which servers and services are dispersed all over the globe in distributed data centres. Fog computing extends cloud computing and services to the edge of the network.

End devices, sensors, RFID tags, and actuators can use controllers that are in the fog. This frees up bandwidth in the network for other uses. These controllers can use Cisco IOx. These IP-enabled controllers are able to forward information across an IP network, and allow individuals to access the controller remotely. Some controllers are able to consolidate information from multiple sensors or perform basic analysis of data received.

Infrastructure devices are primarily responsible for moving data between the controller devices and other end devices across the network.

Sensors must be told what data to capture and where to send that data. A controller must be programmed to receive that data and decide if it should relay a message to another device.

All of these functions rely on programs. A computer program is a set of instructions given to a computer, to be executed in a specific order. Because computers do not speak human languages, computer programming languages were created. These languages allow humans to write instructions in a way that computers can understand.

Session 4: Transitioning to the IoE

4.1 The IoE connections

The IoT is focused on connecting the unconnected, primarily the 'things' of the IoE. Connecting the unconnected requires a convergence between an organisation’s operational technology (OT) and the information technology (IT) systems those organisations have in place.

OT is defined as an organisation's industrial control and automation infrastructure. This includes the hardware (such as sensors and end devices) and the software that is used to control and monitor the manufacturing equipment and processes. Most communication in OT is accomplished between machines.

IT systems refer to the network infrastructure, telecommunications, and software applications that are used to process information and allow the exchange of that information between humans.

Converging IT and OT

By converging IT and OT systems in an IoE solution, organisations can create better products, achieve cost and risk reductions, and improve performance, flexibility and efficiency. Figure 1 shows the control centre of a modern train system that monitors the status of routes and train operations. With IoE solutions, organisations can implement a simple, smart, and secure approach that allows organisations to:

- **Simplify the infrastructure (simple)** – Seamlessly converge IT and OT infrastructure to reduce operational costs and increase process efficiencies.
- **Create intelligence and agility (smart)** − Use application-centric analytics so applications can run at peak performance and gain information from the infrastructure for new services.
- **Deliver end-to-end security (secure)** − The converged infrastructure defends against attacks and responds to threats intelligently and dynamically.

To implement IoE solutions, organisations must examine and account for three distinct connection types: M2M, M2P, and P2P.

Figure 1

4.1.1 M2M connections

Critical components of modern M2M systems include sensors, actuators, and controllers. They must have a network communications link and programming that instructs a device how to interpret data, and based on predefined parameters, forward that data.Figure 2 shows M2M connections working in an auto plant.

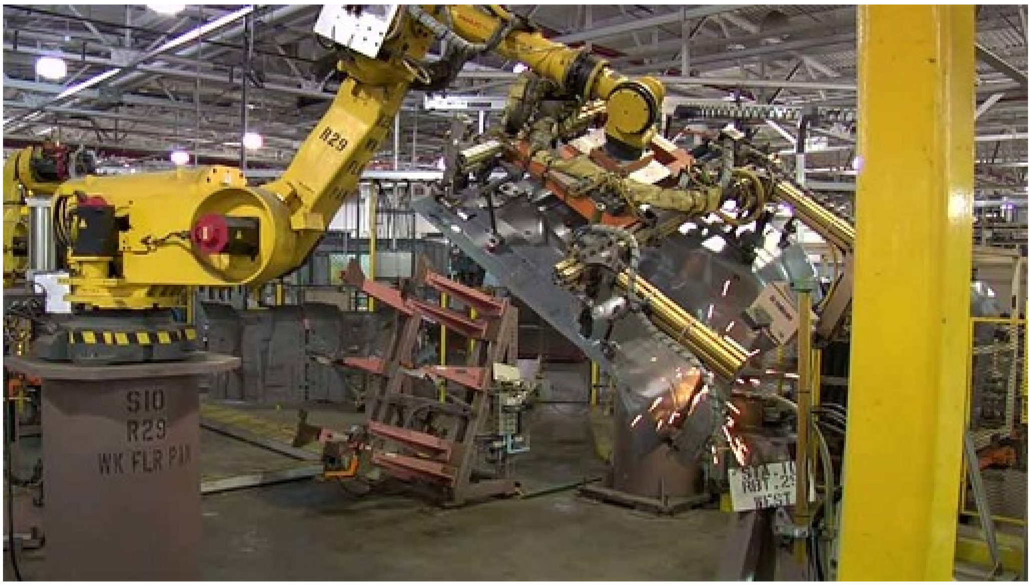


Figure 2

M2M connections are typically present in tracking physical assets, optimizing operations through sensor data and monitoring systems or machines remotely. The most well-known type of M2M communication is telemetry, which is used to transmit performance measurements gathered from monitoring instruments in remote locations. Products with built-in M2M communication capabilities are often marketed as being 'smart products'.

Currently, M2M does not have a standardised connected device platform. These devices communicate using proprietary protocols that are device- or task-specific, and are unable to communicate across other platforms. However, as M2M connections become more prevalent, the need for agreed upon standards will become more crucial.

M2M communication is an important aspect in many industries, including retail, manufacturing, public service and service provider industries. Table 1 provides some examples. As technology continues to evolve, and new connection types become available, new sources of value will emerge.

Table 1 M2M interactions

Sector	Connections	Impacts
Retail	Shelf sensors	Inventory visibility
	Parking-space sensors	Automated ordering process
	Infrared motion sensors	Flexible payment options Energy optimisation
	Weight mats	
	Environmental sensors (light, temperature)	
	Door sensors	
	Mobile payments	
	Energy meters	
Manufacturing	Converged IP factory network	Remote asset monitoring
	Sensors (vibration, HVAC, lighting)	Predictive maintenance
	Actuators	Flexible production
	Sensor-to-ERP connectivity	
	Input/output machines	
	Process operation controls	
	Product packaging	
Public sector	Smart buildings	Improved citizen/employee/student experience
	Smart lighting	Improved asset utilisation
	Smart payments	New revenue streams
	Intelligent public transit	Energy optimisation
	Smart grid	
Service providers	Car sensors	Remote site monitoring Service
	Appliance sensors	Smart commerce
	RFID	Intelligent diagnostics
	Digital billboards	Targeted advertising
	Unused inventory	
	Office facilities	
	Trucks	

4.1.2 M2P connections

People play an important role in harnessing the digital intelligence gathered by M2M connections. The resulting M2P connections are essential for optimal decision making.

For example, portable sensors and monitors can provide round-the-clock information on a patient's vital signs, but health care providers are ultimately responsible for using that information to assess patients and provide treatment.

M2P connections mean that people can send information to technical systems and receive information from these systems. M2P connections are transactional, which means the flow of information moves in both directions, from machines to people and from people to machines. M2M and P2P connections are also transactional.

M2P technologies can range from automated customer notification systems with preset triggers, to advanced dashboards that help people visualise analytics. People can also perform more complex M2P operations such as examining and analyzing received data, and determining how to present information to decision-makers.

In addition to offering improvements in efficiency, the IoE provides safety benefits. For example, sensors in the ground and on the miners make it possible to detect danger signs before an accident occurs. Vibrations in soil and rock, or changes in human vital signs, can prompt real-time M2M or M2P interactions that save property, investments, and lives. Table 2 provides examples of the impact that M2P connections can have in retail, manufacturing, the public sector, and service provider industries.

Table 2 M2P interactions

Sector	Connections	Impacts
Retail	Digital signage	Understand shopper behaviour
	Connected shopping carts	Personalised content
	Video cameras	Endless aisle omnichannel
	Wi-Fi badges	Optimised retail operations>
	Point-of-sale devices	
	Kiosks	
Manufacturing	Video analysis of control systems	Operations analytic
	Operations dashboards	Real-time supply chain
	Safety tags and signage	IT and physical security
	Fleet/logistics systems	
	Partner/supplier supply-chain data	
	Distribution locations	
	IT assets and endpoints	
Public sector	Video surveillance	Enhanced security, safer communities
	Smart parking	Increased revenue/compliance
	Disaster response	Smart public safety fleets
	Inpatient monitoring	
Service providers	Intelligent GPS	Personalised traffic report

	Home security devices Home energy devices Automated customer notifications Auto-translation Sponsored data Connected life	Hyper location presence Health order refills Home security energy control

4.1.3 P2P connections

M2M and M2P connections are an important aspect of any IoE solution. But, for a complete IoE solution, individuals must communicate and collaborate with others using P2P connections.

P2P connections are characterised by collaborative solutions that leverage new and existing network infrastructure, devices, and applications. These optimised and secure network platforms allow for voice, video and data to be presented in a single view, to and from any endpoint or mobile device.

P2P applications provide services for managing meeting room reservations and resources, for example, using Cisco Smart+Connected Meeting Spaces. P2P applications also support online collaboration through web and video conferencing, for example, using Cisco Webex. Table 3 provides examples of the impact that P2P connections can have in retail, manufacturing, the public sector, and service provider industries.

Table 3 P2P interactions

Sector	Connections	Impacts
Retail	Store associate mobile devices Immersive video Social media Contact centre	On-demand expert advice Collaborative product development On-demand training
Manufacturing	Environmentally hardened mobile video device Active collaboration rooms R&D and production teams Engineers and production experts Contact centre Business-to-business (B2B) e-commerce site	Remote Expertise Collaborative Product Development Mobile collaboration on factory floor
Public sector	Telework Bring your own device (BYOD) Connected learning	Employee productivity Lower costs Distance learning

Service providers	Video cameras	Collaboration as a service
	Television	TelePresence as a service
	Digital signage	Smart health
	Social media	
	Contact centre	

4.1.4 M2M, M2P, P2P interacting to form solutions

Implementing an IoE solution using M2M, M2P and P2P connections, provides organisations and individuals with actionable insights and seamless automation.

For example, consider how a business that sells metallic, purple phone covers, might benefit from these interactions should a sudden spike in demand occur. Analytics first pick up indications of this trend for that product and color on social media. That business predicts the change in demand. M2M, M2P, and P2P connections can prompt factories and suppliers to ramp up production of this metallic, purple phone cover.

As IT and OT converge, all aspects of the supply chain are connected. Through wireless sensors and networked mobility, companies gain immediate visibility into every aspect of the product cycle, from initial consumer interest to post-purchase feedback:

- consumer interest informed by checkout process, carts and shelves, post-purchase feedback
- inventory informed by loading docks, stock shelves, and warehouses
- logistics informed by trucks and trains
- production informed by factory floors and machines.

Table 4 shows how the interaction of the devices and people might occur.

Table 4 Interaction process

Step 1	Step 2	Step 3	Step 4	Step 5
Customers talk to companies through purchase habits and online feedback.	Companies talk to supply chain management channels.	Supply chain management systems talk to machines on the factory floor.	Machines on the factory floor talk to the suppliers of raw materials.	Suppliers of raw materials inform supply chain management channels of the shipment of raw materials.

With IoE, there is the potential of providing connections all the way back to the mines and drilling operations, where raw materials are extracted from the ground. Those mines, which are the start of the production value chain, illustrate the IoE’s value, particularly its ability to offer predictive insights.

4.2 Implementing an IoE solution

In this section you will be introduced to how you may design and implement an IoEsolution. There are many challenges and each system has its own requirements which must be considered. In reading this section, you will explore bandwidth and technology growth considerations, how proprietary (manufacturer specific) systems affect any IoE solution, the processes required for connecting different systems, how you may adjust different technologies.

4.2.1 Understanding existing business processes

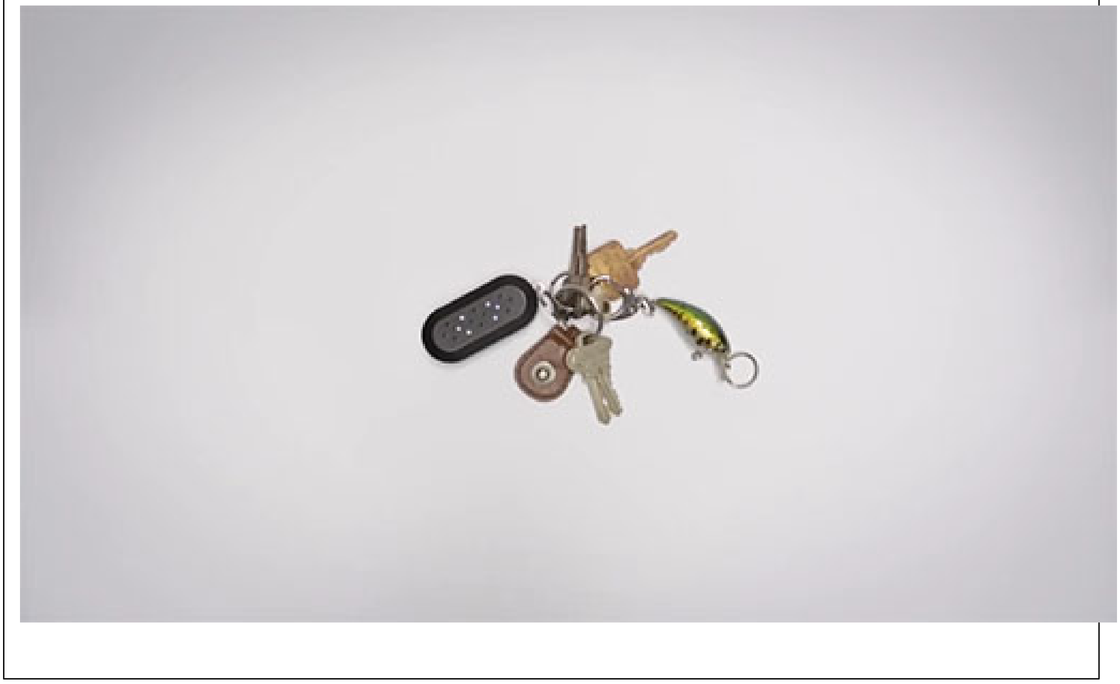
Implementing an IoE-enabled business model can improve business operations, save costs, and allow for more effective marketing strategies. But how can an organisation implement new IoE solutions without disrupting current operations?

One of the first steps business managers must take is to understand their current processes. They must identify:

- Who their suppliers and customers are
- What customer needs are
- What the schedule and process steps are for creating and delivering an offering

For example, as a supply manager or distributor, it is important to understand when receipt of an item will be in relation to the expiration dates of those same products. Watch this video of the supply chain feedback loop for banana harvests.

Video content is not available in this format.



4.2.2 Understanding existing IT and OT networks

In addition to understanding business processes, organisations that are implementing an IoE solution must consider the existing IT and OT network infrastructures and operations.

Business managers must understand how the IT network users interact with the network resources and services and gather information about all internal and external access to the existing network infrastructure. Without full knowledge of who has access to the network and how it is used, the intended solution might not include some user requirements, or incorrectly identify user groups. Other considerations include identifying the existing network and infrastructure components, and capabilities, including support for traffic requirements, data storage, and security needs.

In addition to understanding IT network operations, business managers must also consider how current networks of OT systems operate. This includes knowing how the M2M connections currently take place, the information that is generated from these connections, and how this information is integrated into the current business processes. They must also identify any connectivity requirements, such as the use of proprietary protocols.

4.2.3 Business goals and opportunities

Business managers must also take into consideration business goals, business styles, tolerance to risk, and the level of technical expertise available. Business managers must analyse the feasibility of an IoE project based on how it contributes to business success. Considerations might include:

- **Profitability** − Determine cost and return on investment of implementing the IoE project as a result of efficiencies and improvements.
- **Business growth and market share** − Identify growth opportunities and competitive advantages due to the IoE implementation as a result of new insights.
- **Customer satisfaction** – Determine the impact to customer experience and loyalty as a result of improved responsiveness to customer needs.

4.2.4 Cisco streamlines old mining operation

A full IoE implementation is an end-to-end solution with multiple M2M, M2P and P2P connections. Companies must determine implementation priorities based on those connections that provide the best opportunity to contribute to the success of the business.

Consider how a mining company might use IoE solutions to optimise operations and reduce costs by asking:

- What benefits can an IoE solution bring to a mining organisation?
- How can the organisation be impacted by the real-time data?
- How is cost-saving achieved by the IoE implementation?
- What types of profits could be foreseen by the owners, shareholders, and employees?

- While there are many connections that can be made in the IoE solution, which ones will provide the best return on investment (ROI) and, therefore, should take prioritisation?

Watch the video to see how mining companies use IoE to provide connectivity and collaboration across the organisation and the systems they use. A focus of the video is one IoE solution that was implemented to minimise downtime of trucks used in operations, which can save money.

Video content is not available in this format.

4.2.5 Determine technical requirements

!Warning! CiscoSansTTLight,Helvetica,Arial,sans-serif not supportedAfter business managers have determined their priorities and established the changes in business processes that must be made, the technology professionals can then begin the process of determining the technical requirements. Table 5 provides more information.

Table 5 Technical requirements

Standardisation	Equipment	Network scalability	Security	Network management	Programming	Data processing and access
What technology is required to allow these systems to communicate to IT systems, or to convert these systems to use IP?	What new equipment is required? Are sensors needed to track information? What devices are needed to aggregate	How does the existing infrastructure need to be modified to support the new technical requirements and data load?	What security measures need to be implemented on IT systems, OT systems, and end devices?	Does the new device integration create a more complex network environment? If so, what new services and	What are the programming requirements needed to support non-IP-enabled and IP-enabled devices?	When is it necessary to forward data to the Cloud for processing, and when does data need to be processed

	information and help with information management?	applications need to be installed to simplify the management of these updated systems?	closer to the source, for example, in the Fog?

4.2.6 Potential constraints

Constraints can and do affect IoE implementations and should be identified early when implementing a solution. The relative importance of the constraints varies from project to project. Budget constraints are not always the main consideration for a large project (Table 6).

Table 6 Potential contraints

Budget	Legacy systems	Technical expertise	Policies	Culture
Limited resources may require some compromises in design due to the costs of equipment, software, or other components.	Businesses may have large capital investments in existing systems.	The lack of trained personnel to implement an IoE solution is a major constraint.	The design must account for existing policies regarding protocols, standards, vendors, and applications. If necessary, these policies need to be refined or removed. In some cases, new policies must be created to facilitate the IoE implementation.	The change over to an IoE implementation requires a collaborative environment with open communications between traditionally segmented departments.

In addition to these common constraints, business managers must also consider the complexity of any existing IT and OT designs when converging IT and OT in the new IoE implementation.

4.2.7 The IoE architectural approach

Cisco's architectural approach to the IoE is organised into three functional layers. The application layer is dependent on the platform layer, which is dependent on the infrastructure layer (Table 7).

Table 7 Architectural approach

Application layer	Platform layer	Infrastructure layer
This layer provides automated, dynamic,	This refers to Cisco solutions that provide orchestration,	This layer integrates power, security, core networks,

application-centric responses to changing traffic and usage demands. The application layer includes the intelligence needed to improve user experiences. It allows for the integration of traditional IT apps, and the use of collaboration applications and industry-specific applications.	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 complicated 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.	access architectures, and storage with physical and virtual resources. It includes the right mix of hardware and software across enterprise, Cloud, and service provider networks. It converges all connections, both OT and IT, into IP and accounts for Cloud computing and mobile connectivity.

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), andiInfrastructure as a service (IaaS).

4.2.8 Adjusting technologies

Organisations must adjust the technologies that are used across the infrastructure and applications. The table provies more information.

Table 8 Adjusting technologies

Standard infrastructure	Responsive software	Holistic security
This refers to establishing and implementing standardised protocols and coordinating services in an end-to-end IP environment. This helps reduce, or eliminate, the costs associated with legacy systems. It also creates seamless integration across autonomous departments, which allows for increased collaboration, rapid delivery of information, and end-to-end management and security.	This requires, through an application-centric approach, enabling the infrastructure to automatically and rapidly detect, and adapt to, traffic demands and flows. This allows the infrastructure to react to changing conditions and potential issues, without compromising security or availability. A large part of an application-centric approach is establishing what information is virtualised, what moves into the Cloud, and what stays within the Fog.	This refers to securing a network infrastructure from end-to-end. It includes enabling technologies that can monitor network operations and automatically detect and mitigate threats. It simultaneously ensures confidentiality, integrity, and availability of any information that is transmitted across the network.

4.2.9 Connecting processes

The Process pillar describes how people, data, and things interact with each other to deliver societal benefits and economic value. By connecting the unconnected, we have visibility into new processes, providing opportunities to create more efficient and effective interactions. Cisco is working with major retailers to use a combination of sensors, video, and analytics to improve store productivity and customer experience.

Watch this video about how the IoE affects a users' trip to a US-based online store (Big Box).

Video content is not available in this format.

4.2.10 The IoE in retail

When transitioning to an IoE model, retailers have the opportunity to create new and better connections in their stores, corporate offices, distribution centers, and other environments. Figure 3 compares retail examples of the past with the IoE. Click on each of the terms on the left to see more information. Press each button to reveal a different section of the IoE retail infrastructure.

Interactive content is not available in this format.

Figure 3

4.2.11 The IoE in manufacturing

Before IoE, manufacturers had little contact with customers and it was time-consuming to collect customer feedback on products. IT and OT operations were also separate.

With IoE, products and services can include embedded sensors that provide manufacturers with constant data and feedback. IT and OT operations are converged (Figure 4). Press each button to the left to reveal a different section of the IoE manufacturing infrastructure.

Interactive content is not available in this format.

Figure 4

4.2.12 The IoE in the public sector

Creating new and better connections, and collecting information from assets, can pay enormous dividends for governments (Figure 5). Press each button to the left to reveal a different section of the IoE public sector infrastructure.

Interactive content is not available in this format.
(Figure 5)

4.2.13 The IoE for service providers

IoE opens up tremendous possibilities for service providers to monetise their network. Service providers already have large networks that deliver mobile, video, collaboration, and other offerings to individual subscribers and businesses of all sises. They can now integrate many types of IoE connections to deliver rich new services (Figure 6). Press each button to the left to reveal a different section of the IoE service provider infrastructure.

Interactive content is not available in this format.
Figure 6

4.2.14 Proprietary ecosystems

To achieve a complete IoE solution, interoperability is critical. OT networks and systems are often implemented using proprietary protocols that may be insecure. These protocols do not interoperate well with the protocols of an IP network, which are typically more secure.

One of the first steps is to develop a solution that allows the devices to speak the same language, regardless of the vendor. One way to accomplish this is to convert proprietary networks to IP-based networks. Another approach is to ensure that these proprietary protocols can communicate through a translator.

4.2.15 Technological growth

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

There are three primary principles, referred to as laws that organisations 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.

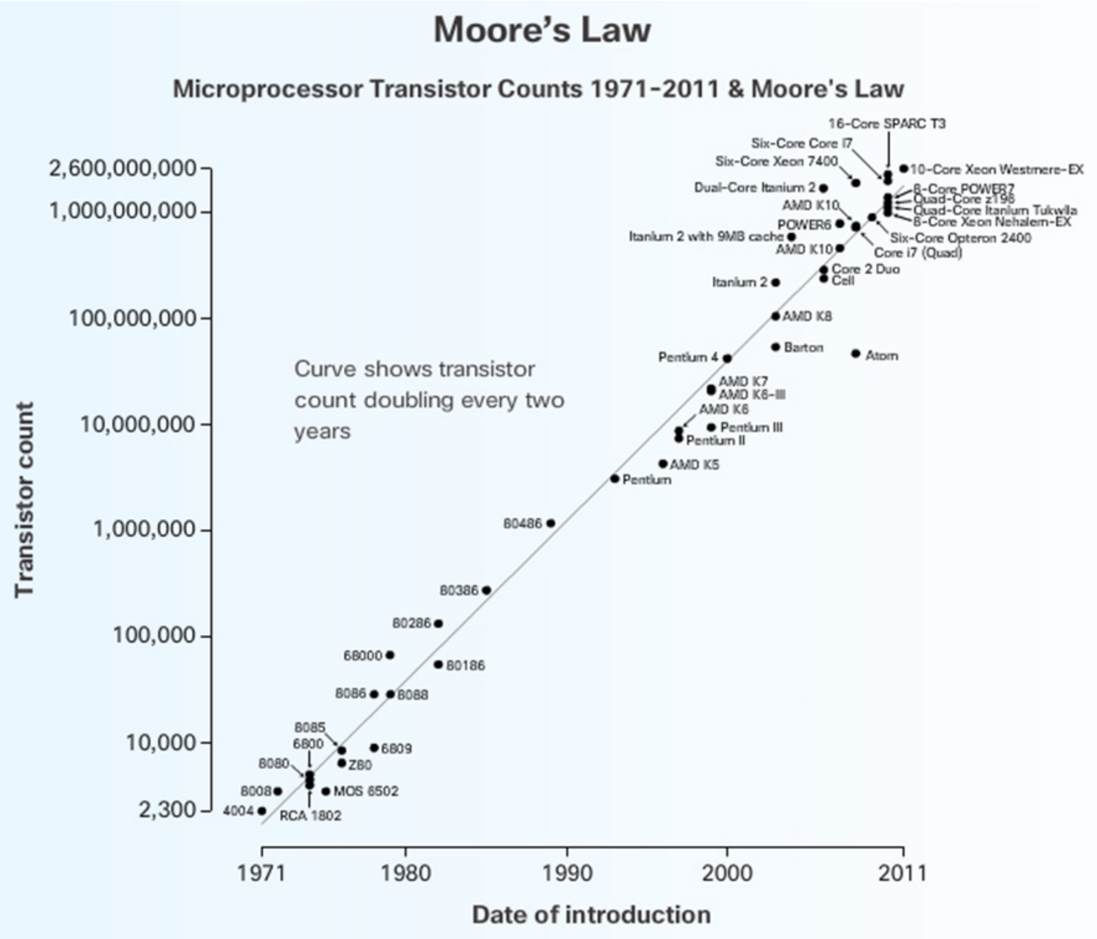
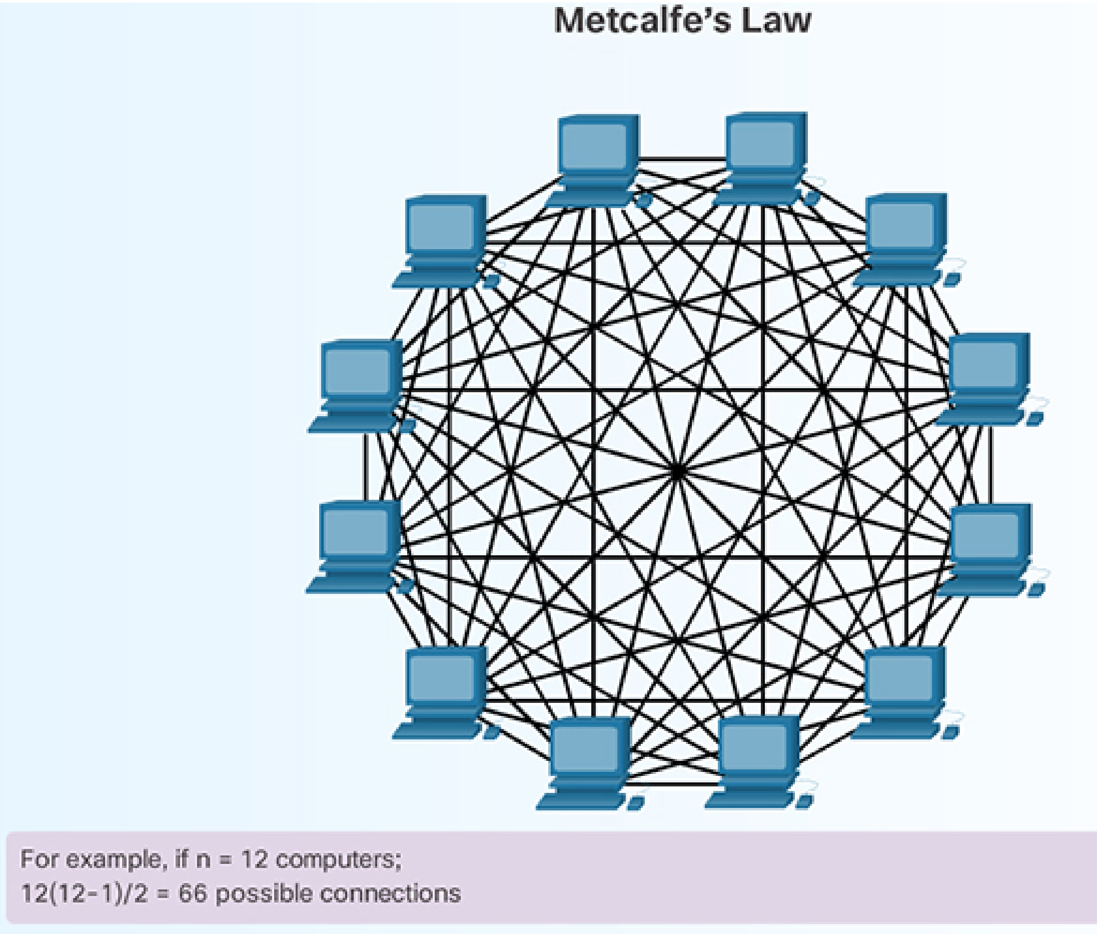


Figure 7

- **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. As shown in Figure 78 Metcalfe's Law relates to the number of unique connections in a network of (n) nodes, mathematically expressed as n(n−1)/2. The value described by this law is therefore proportional to n^2.



Metcalfe's Law

For example, if n = 12 computers;
12(12-1)/2 = 66 possible connections

Figure 8

- **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. This is represented as 2^n and is best seen with social media networks.

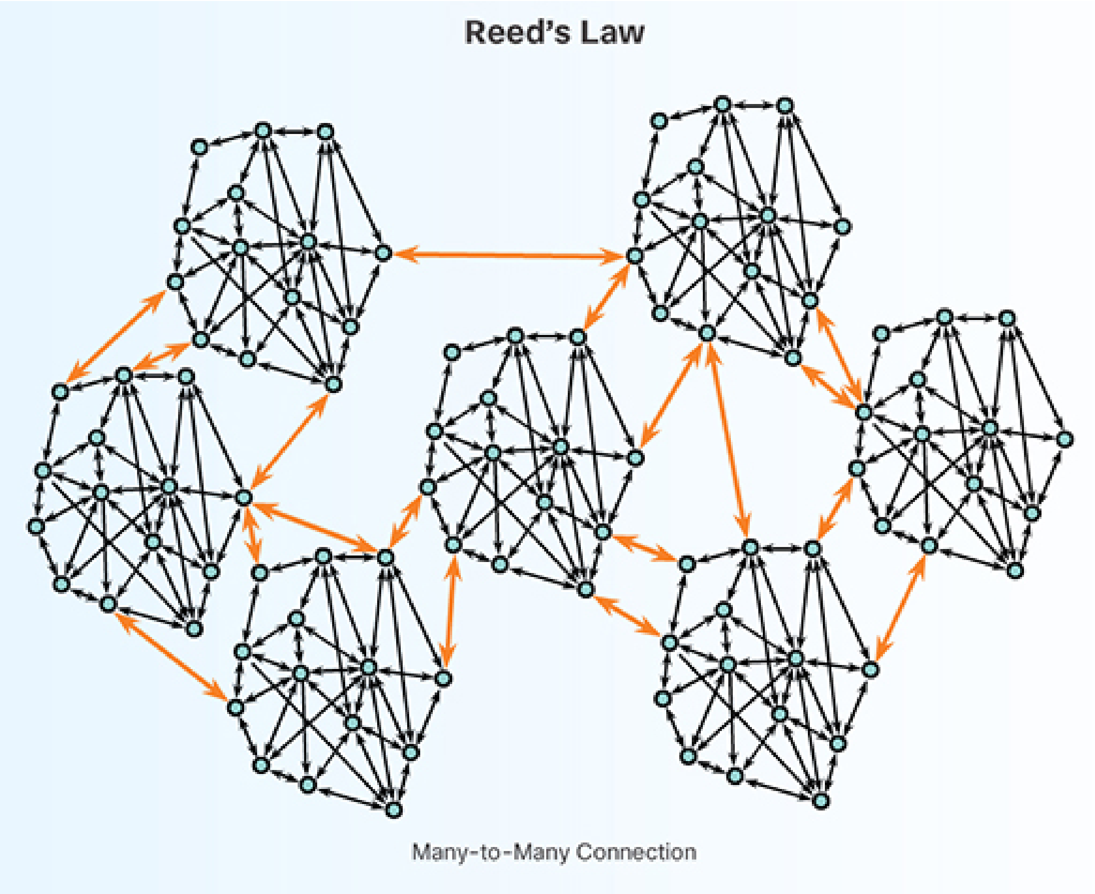


Figure 9

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.

4.2.16 Growth relevance to IoE

Moore's law allows organisations to make a rough estimate as to the computing power of machines in the future. The exponential growth in computing power allows us to make an estimate as to how long before the technology is ready and available at a reasonable cost to consumers. This allows organisations to not only plan for their own technological advances, but also to predict the advances of their competitors.

Metcalfe's law is useful for business managers to calculate the optimal number of interconnections between nodes. They must complete a cost-benefit analysis because the number of connections increases both costs and benefits.

When the cost of sensors used in the IoE becomes low enough, the benefits of more meshed networks are realised. Currently, most IoE implementations rely on controllers and gateways to aggregate the traffic between IoE end devices. These types of IoE devices incorporate many-to-many designs, as described by Reed’s law.

These principles allow organisations to better predict and plan for future needs and opportunities.

4.2.17 Big data challenges

The exponential growth of data continues as the number of things connected to the Internet increases. However, more data is not necessarily better if that data cannot be accessed, analysed, and applied in a usable manner. For data to be a true asset, it must be used effectively. In addition, using old, inaccurate data wastes time, resources, and money.

Managing this increased amount of data creates many challenges, including:

- bandwidth capacity on existing links connected to data centres
- privacy concerns for user data
- managing data for real-time communications
- selecting and analysing appropriate data.

Insights from Big Data will enhance customer engagement, improve operations, and identify new sources of value. However, the increasing demands of Big Data require new technologies and processes for data centers and data analysis.

4.2.18 Bandwidth requirements

As more and more things are connected to the Internet, the demand for bandwidth will increase because of M2M communications in industrial, government, and home applications.

Fifty sensors may not consume much of your home’s Wi-Fi bandwidth simply because each device intermittently bursts a small amount of data. However, 50 sensors could be a very conservative estimate of the number of things connected per home in the next decade.

An essential characteristic of cloud computing is broad network access. In cloud computing service models, enabling on-demand network access to shared computing resources and services over the network results in increased requirements for network bandwidth. In turn, higher bandwidth requirements demand infrastructure improvements.

4.2.19 Cloud vs fog computing

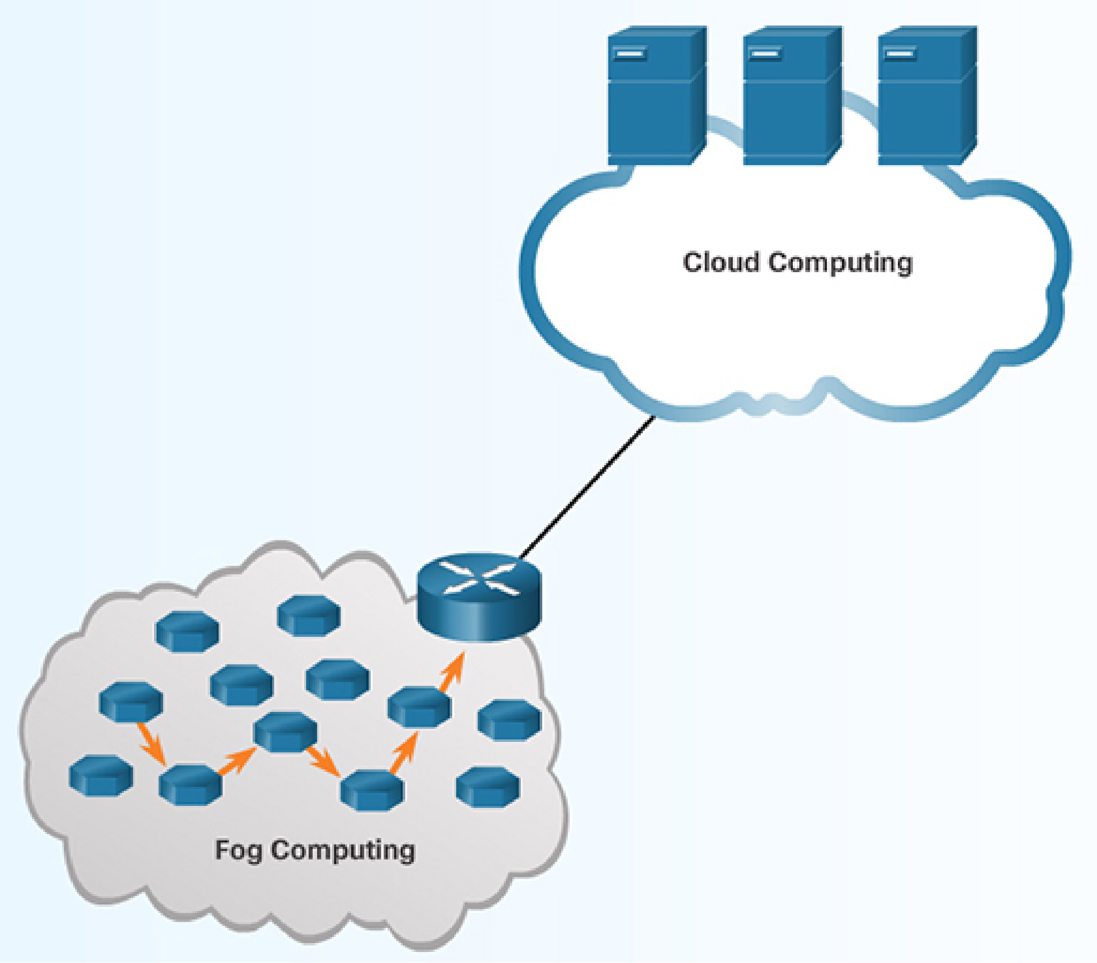


Figure 10

Cloud computing solutions will create substantial increases in bandwidth needs as data and services are moved and processed in the Cloud, promoting organisational flexibility and agility.

However, some data and service solutions are more appropriate closer to the source. For example, smart light traffic systems require real-time processing. The selected computing model must enable the level of resiliency, scale, speed, and mobility that is required to efficiently use the data.

To deliver the best value, system designers must consider the distribution of data and account for different computing models. As a result, some services and applications may need to move from the cloud into the fog. This can help manage escalating bandwidth needs.

4.2.20 The learning society

!Warning! CiscoSansTTLight,Helvetica,Arial,sans-serif not supportedPeople are the most valuable asset in any organisation. To remain relevant and competitive in any environment, training must be a top priority. The impact of the IoE will affect all aspects of an organisation's operations. As a result, the entire organisation will require training to take advantage of IoE opportunities. For example, OT and IT must work together in innovative ways to overcome the challenges and realise the benefits of the IoE.

4.3 Security and the IoE

Security has become the primary concern for all interconnected computer systems. The IoE is not immune to attack and a good system should be designed with security in mind. In this section you will cover security architecture and policies, what may be a beneficial security strategy, the pervasive nature of security, security devices, wireless security, the risk of personal data with the IoE and system redundancy and how this assures security.

The increased number of connected devices and the amount of data they generate increases the demand for security of that data.

Watch the video of John Stewart, Senior Vice President, Chief Security Officer at Cisco Systems, discussing how to secure billions of devices in the IoE.

Video content is not available in this format.

Hacking attacks are a daily occurrence, and it seems no organisation is immune. Given how easy it is to steal and misuse information in today's connected world, it is only natural to be concerned about this problem as people, process, data, and things all become connected in the IoE. In the video, DARPA and Car Hacking, Dr. Kathleen Fisher of the Defense Advanced Research Projects Agency (DARPA) describes how a hacker could control the operation of a motor vehicle remotely.

4.3.1 Security strategy

The larger and more integrated the IoE solution, the more decentralised the network becomes. This allows for a greater number of access points into the network, which introduces a greater number of vulnerabilities. A significant number of the devices communicating across the IoE will be transmitting data from insecure locations, but those transmissions must be secure. However, securing an IoE solution can be difficult due to the large number of sensors, smart objects, and devices that are connected to the network. The potential harm caused by allowing unsecured devices to access an organisation's network is a significant challenge for security professionals.

So how does an organisation or individual leverage the benefits of the IoE while managing risk? Take a look at Table 9.

Table 9 Security strategy

Adaptable and real-time security	Secure and dynamic connections	Protecting customer and brand trust
Prepare to handle security as you grow by deploying adaptable and real-time security. As business evolves, adjust security levels to minimize risk.	Ensure that the right level of security is in place for all connections all the time. Advanced security measures and protocols help achieve regulatory and privacy compliance. All valuable assets including intellectual property, data, employees, and buildings are protected.	Reduce the impact and cost of security breaches with a seamless security strategy. Security breaches erode customer confidence and brand integrity. The security strategy must detect, confirm, mitigate, and remediate threats across the entire organisation.

4.3.2 Pervasive

Currently, network security is largely driven by the effort to stay ahead of threats. Just as medical doctors attempt to prevent new illnesses while treating existing problems, network security professionals attempt to prevent future attacks while minimising the effects of successful attacks.

Within the IoE, security must be pervasive. The approach to security must be:

- consistent, automated, and extend to secured boundaries across organisations
- dynamic, to better recognise security threats through real-time predictive analytics
- intelligent, providing visibility across all connections, and elements of the infrastructure
- scalable, to meet the needs of a growing organisation
- agile, able to react in real-time
- comprehensive, end-to-end solution.

A pervasive security solution avoids disjointed security implementations that can increase complexity, be difficult to manage, and require increased staffing and technical knowledge to support.

4.3.3 Security architecture

Securing IoE networks cannot be about securing just the individual devices. Rather, it is about implementing an end-to-end security solution.

A security solution that provides protection with centralised policy management and distributed enforcement must be integrated throughout the network. Continuous monitoring of activity on the network is needed to aggregate and correlate data across the connected environment, leveraging insights, and taking action as needed.

Cisco’s security architectures use infrastructure, platform, and application layers to provide a comprehensive set of tools and systems. These tools and systems work together to produce actionable security intelligence, in near real-time, while allowing the network to adjust to security threats with little or no human intervention required (Table 10).

Table 10 Security architecture

Access Control	Context-aware policies	Context-aware inspection and enforcement	Network and global intelligence
Access control provides policy-based access for any user or device seeking access to the distributed network. Users are authenticated and authorised. End devices are also analyzed to determine if they meet the	Context-aware policies use a simplified descriptive business language to define security policies based on the full context of the situation: who is sending, what information, when, where and how. These security	Context-aware inspection and security enforcement use network and global intelligence to make enforcement decisions across the network. Flexible deployment options, such as integrated security services, standalone	Network and global intelligence uses the correlation of global data to ensure that the network is aware of environments that have a reputation for malicious activity. It provides deep insights into network activity and threats for fast and accurate

security policy. Non-authenticating devices, such as printers, video cameras, sensors, and controllers are also automatically identified and inventoried.	policies closely align with business policies and are simpler to administer across an organisation. They help businesses provide more effective security and meet compliance objectives with greater operational efficiency and control.	appliances, or cloud-based security services bring protections closer to the user.	protection, and policy enforcement.

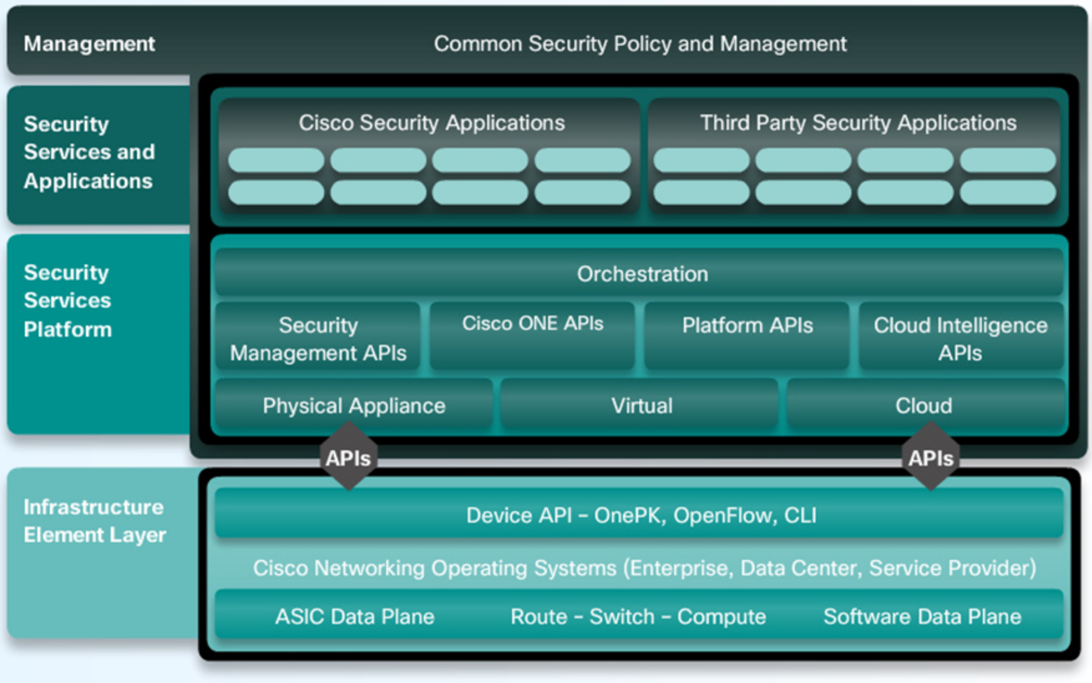

Management
Common Security Policy and Management
Security Services and Applications
Cisco Security Applications
Third Party Security Applications
Security Services Platform
Orchestration
Security Management APIs
Cisco ONE APIs
Platform APIs
Cloud Intelligence APIs
Physical Appliance
Virtual
Cloud
APIs
APIs
Infrastructure Element Layer
Device API – OnePK, OpenFlow, CLI
Cisco Networking Operating Systems (Enterprise, Data Center, Service Provider)
ASIC Data Plane
Route – Switch – Compute
Software Data Plane

Figure 11

Figure 11 shows a Cisco security architecture. The security principles described in the table above are applied across the layers of the architecture. The architecture includes the infrastructure layer at the bottom, which provides a set of application programming interfaces (APIs). These APIs deliver certain functions and applications to the security services platform layer above. At the top of the platform sits a common security policy and management layer that manages the entire platform.

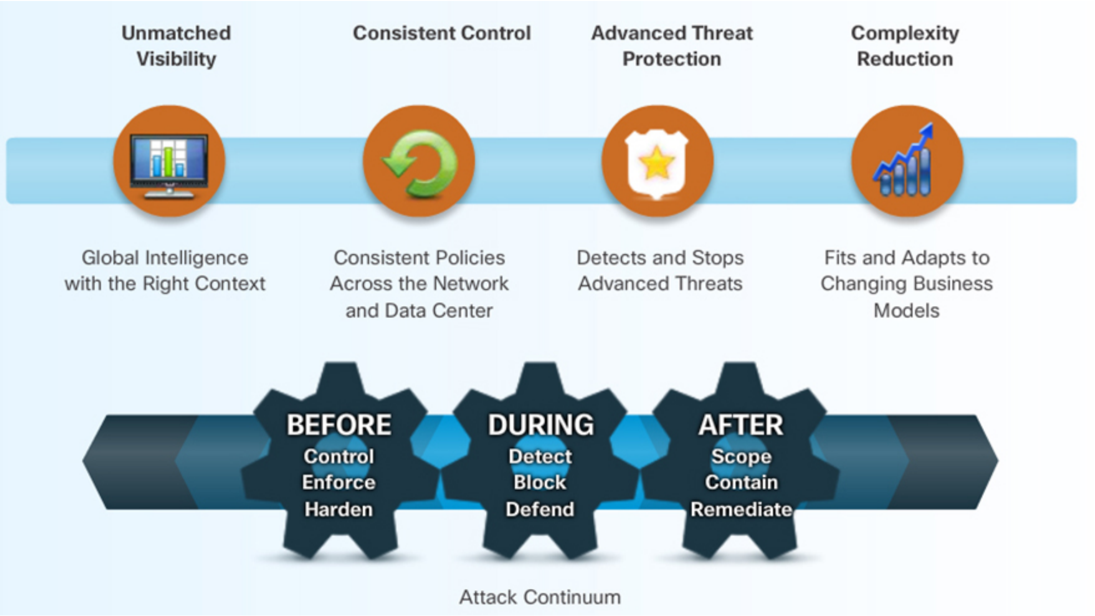

Unmatched Visibility
Consistent Control
Advanced Threat Protection
Complexity Reduction
Global Intelligence with the Right Context
Consistent Policies Across the Network and Data Center
Detects and Stops Advanced Threats
Fits and Adapts to Changing Business Models
BEFORE
Control
Enforce
Harden
DURING
Detect
Block
Defend
AFTER
Scope
Contain
Remediate
Attack Continuum

Figure 12

Implementing a Cisco security architecture provides the benefits shown in Figure 12, as well as continuous support before, during, and after a security event or attack.

Cisco is uniquely positioned in the IoE market. As a pioneer in the security industry, Cisco has end-to-end solutions within its product lines.

4.3.4 Security devices

Some of the devices in the security architecture that can be used to control access, inspect content, and enforce policies include:

- **Firewalls** – A firewall creates a barrier between two networks. The firewall analyses network traffic to determine if that traffic should be allowed to travel between the two networks based upon a set of rules that have been programmed into it, as shown in the following animation. (Click on the full screen button for a clearer view.)

Video content is not available in this format.

- **Intrusion prevention systems (IPS)** − The IPS monitors the activities on a network and determines if it is malicious. An IPS will attempt to prevent the attack by dropping traffic from the offending device or resetting a connection. Figure 22 shows more about how an IPS works.

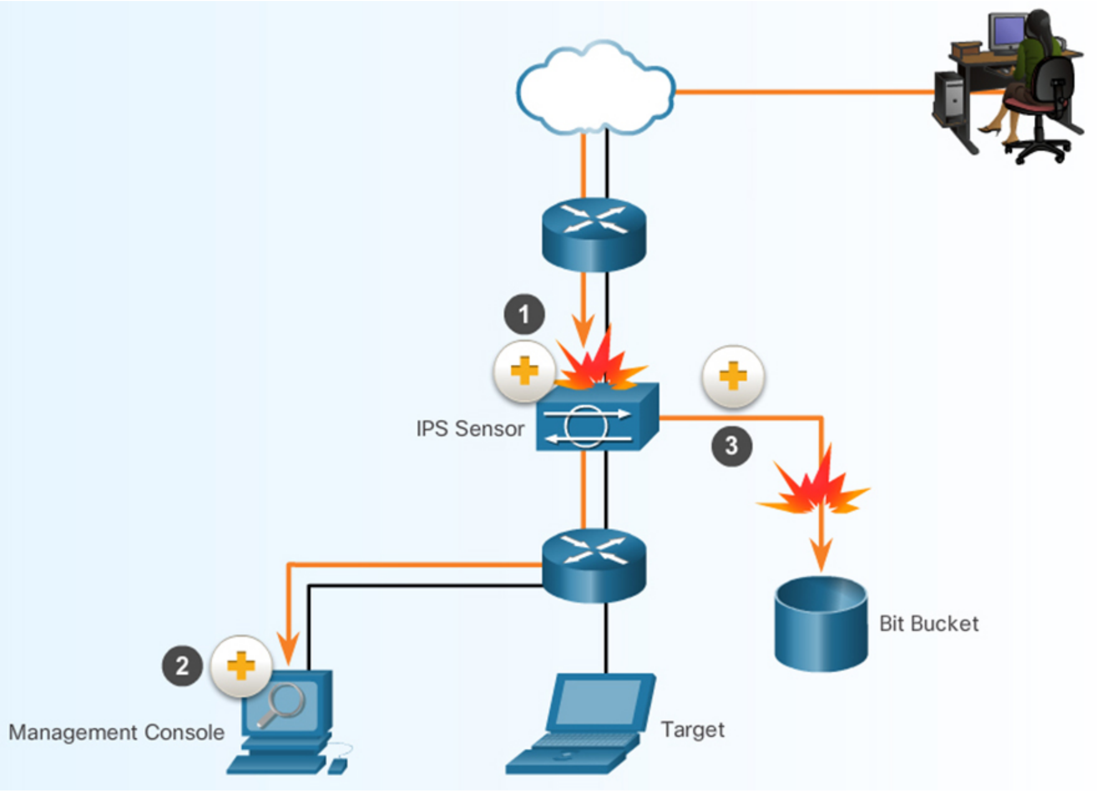


Figure 22

4.3.5 Application-centric security

As organisations move to application-centric environments, the traditional security solutions are no longer adequate. Cisco’s ACI Security Solutions protect environments by fully integrating customised security technologies for the needs of a specific application. ACI Security Solutions can be managed as a pool of resources that are attached to applications and transactions using a central controller. This solution can automatically scale on demand providing seamless policy-based security.

This solution allows for a holistic, policy-based approach to security that reduces cost and complexity. It integrates physical and virtual security technologies directly into Cloud and datacenter infrastructures.

Watch the video overview of the Cisco ACI.

Video content is not available in this format.

4.3.6 Wireless security

The difficulties in keeping a wired network secure are amplified with a wireless network. A wireless network is open to anyone within range of an access point and the appropriate credentials to associate to it.

Wireless security is often implemented at the access point, or the point where the wireless connection enters into the network. Basic wireless security includes:

- setting strong authentication protocols with strong passwords
- configuring administrative security
- enabling encryption
- changing all default settings
- keeping firmware up-to-date.

However, even with these configuration settings, with a wireless-capable device and knowledge of hacking techniques, an attacker can gain access to an organisation's or an individual's network. Additionally, many new wireless-enabled devices that connect to the IoE do not support wireless security functionality.

For this reason, traffic from smart wireless and mobile devices, and traffic from sensors and embedded objects, must pass through the security devices and context-aware applications of the network.

4.3.7 Redundancy and high availability

With so many connections to the network, it is important to ensure that the network is available and reliable.

Redundancy requires installing additional network infrastructure components, telecommunication links, and power components to back up primary resources in case they fail.

Redundancy also enables load sharing of resources, providing a high-availability system design that ensures that a prearranged level of operational performance will be met during a contractual measurement period.

In addition to having redundant equipment and connections, data must also be backed up. Secure backups archive the data in an encrypted format, preventing unauthorised access to the stored archive.

Examples of network redundancy include:

- redundant servers
- redundant fibre connections
- redundant power supplies.

4.3.8 Security policy

!Warning! CiscoSansTTLight,Helvetica,Arial,sans-serif not supportedSome people have malicious intent, while others make mistakes or follow unsecure practices, putting equipment and data at risk. To protect assets, rules and regulations must be put in place to define how users should act, what actions are right or wrong, what they are allowed to do, and how they access systems and data.

A security policy defines all of the rules, regulations, and procedures that must be followed to keep an organisation, its people, and systems secure. A security policy can be divided into many different areas to address specific types of risk (Table 11).

Table 11 Types of security policies for people

Remote access policy	Information privacy policy	Computer security policy	Physical security policy	Password policy
Defines who can connect, how they can connect, when they can connect, and what devices can be used to connect to a system remotely. This policy also defines the assets that are accessible to a remote user.	Defines what methods are used to protect information depending on the level of sensitivity. Generally, the more sensitive the information, the greater the level of protection used to secure it.	Defines the way in which users are allowed to use computers. This policy might define who can use certain computers, what programs must be used to protect a computer, or if a certain storage media is allowed to be used.	Defines how physical assets are secured. Some assets may need to be locked away at night, kept in a locked area at all times, or specifically designated not to leave the property.	Defines what password will be used to access specific resources and the complexity of the password. Often, this policy will control how often a password must be changed.

The most important part of a security policy is user education. The people governed by the security policy must not just be aware of this policy; they must understand and follow it to ensure the safety of people, data, and things.

To learn more about security polices, visit the SANS website.

4.3.9 Personal data and the IoE

Table 12 Categories of personal data

Volunteered data	Inferred data	Oserved data
Volunteered data is created and explicitly shared by individuals, such as social network profiles.	Inferred data, such as a credit score, is based on analysis of volunteered or observed data.	Observed data is captured by recording the actions of individuals, such as location data when using cell phones.

Organisations can collect all sorts of personal data; however, there is a legal and ethical struggle between access and privacy. Blocks of data are enhanced with metadata that includes information about where the data was created, who created it, and where it is going. In this way, data becomes property that can be exchanged. This change will allow personal information to be audited to enforce policies and laws when issues arise.

The definition of personal data, however, is evolving. What might be personal data to one person may not seem like personal data to another person. For example, a cancer patient and a healthy patient may have very different ideas on what medical information they want kept private.

4.4 Terms and concepts practice

This activity will help you to test some of the terms and concepts you've been introduced to.

operational technology

information technology

telemetry

bandwidth

fog computing

firewall

redundancy

security policy

interoperability

Match each of the items above to an item below.

an organisation's industrial control and automation infrastructure

the network infrastructure, telecommunications, and software applications that process information and allow the exchange of information between people

transmission of performance measurements gathered from monitoring instruments in remote locations

the number of bits of data that can be transmitted across a communication link within a given unit of time

extends cloud computing and services to the edge of the network

analyses network traffic to determine if it should be allowed to travel between two networks based upon a set of rules

a technique of installing network components, such as servers, switches, routers, and telecommunication links to back up primary resources in case they fail

defines all of the rules, regulations, and procedures that must be followed to keep an organisation, people, and systems secure

devices can communicate with one another by using the same protocol or a translator device

4.5 Session 4 quiz

Check what you have learned in Session 4.

Session 4 quiz

Use 'ctrl' (cmd on a Mac) or right-click to open the quiz in a new window or tab then come back here when you're finished.

4.6 Summary

The IoE requires a convergence between an organisation’s OT and the IT systems those organisations have in place.

M2M refers to any technology that enables networked devices to exchange information and perform actions without the manual assistance of humans. In M2P connections, technical systems interact with individuals and organisations to provide or receive information. P2P connections are collaborative solutions that leverage the existing network infrastructure, devices, and applications, to allow seamless communication and collaboration between people. Each of these types of connections is transactional.

One of the first steps in implementing an IoE solution is to understand current processes and procedures. In addition to understanding business processes, consider the existing IT network infrastructure, network operations, and network management tools.

Security must be able to react in real-time, so it must be high-performance and scalable. Cisco’s security architecture provides a comprehensive set of tools and systems that work together to produce actionable security intelligence, in near real-time, while allowing the network to adjust to security threats with little or no human intervention required.

A security policy defines all of the rules, regulations, and procedures that must be followed to keep an organisation, people, and systems secure.

The definition of personal data is evolving.

Session 5: Bringing it all together

5.1 Modelling an IoE solution

One of the fastest developing areas in the application of the IoE is in healthcare. While there are many other solutions. This case study gives an excellent insight into how one common need for all of humanity can be improved by the use of pervasive technologies on the IoE.

!Warning! CiscoSansTTLight,Helvetica,Arial,sans-serif not supportedThe IoE is already improving the healthcare industry. The video demonstrates how the IoE is being used in every aspect of healthcare.

Video content is not available in this format.

5.1.1 A diabetic patient healthcare solution model

To demonstrate how the IoE is improving patient care, we will focus on a patient with type 1 diabetes. Type 1 diabetes is a disease where a person's body does not produce insulin, a hormone needed by the body's cells so that the cells can absorb glucose. The glucose is used by the cells for energy. Without enough insulin, glucose builds up in the blood, and cells starve for glucose. This is known as hyperglycemia. With too much insulin, the body burns too much glucose. This is called hypoglycemia. Very high or very low glucose levels can lead to a diabetic coma, where a patient becomes unconscious, and can die if left untreated. People with type 1 diabetes must diligently monitor the levels of glucose in their bodies. They may need to administer proper amounts of insulin to maintain a healthy level of glucose in their blood.

To illustrate a healthcare solution model we will examine John Doe. John Doe is 55 years old. He was diagnosed with diabetes 5 years ago, and has difficulty maintaining healthy glucose levels. He has a record of hospitalisation and diabetic coma. John has recently begun using a health monitoring company (HMC) to help him avoid diabetic comas and emergency visits to the hospital. He wears a continuous glucose monitoring (CGM) device and a fitness tracker to monitor his exercise level and respiration. These devices provide the data for the health monitoring company to determine when his state of health moves outside his normal range.

When John's health data is showing dangerous patterns like those that he has exhibited in the past, the health monitoring company sends John an alert on his smartwatch, smartphone, tablet, and television. The alert tells John to call the health monitoring company so that they can assess his condition. If John still does not change his behavior, and he continues this trend, the health monitoring company will dispatch a mobile patient treatment center (MPTC) to administer urgent care.

5.1.2 M2M interactions

The diabetic healthcare solution model is an IoE solution that can serve as a prototype for other health monitoring companies. When developing an IoE solution, it is important to design a model before creating a prototype.

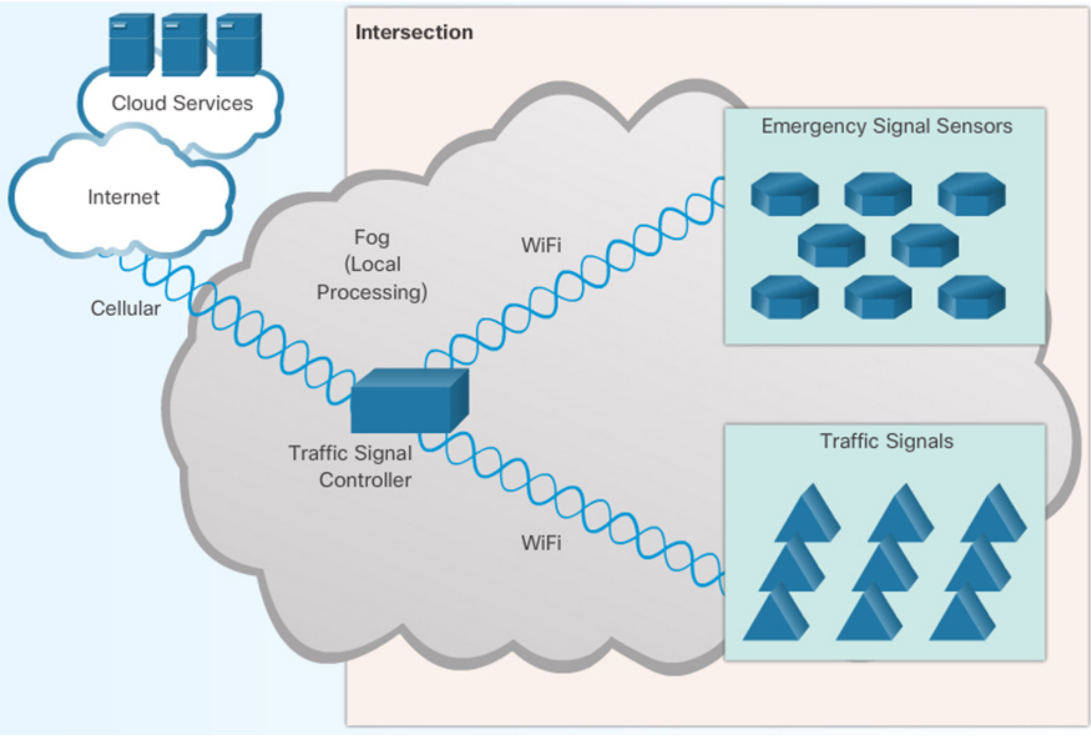


Figure 1

Modeling an IoE solution begins by understanding the potential M2M, M2P, and P2P interactions. Figure 1 shows an initial model of traffic signal control for the health monitoring company's mobile patient treatment center. When sensors indicate that a mobile patient treatment center is approaching an intersection, and the signal is red, the signal is changed to green to allow the mobile patient treatment center to reach John faster. This decision does not need to be made by a person, nor does the required information (to make the decision) need to be sent to the cloud. Data concerning traffic patterns, congestion, and emergency signal interruptions are sent to the cloud for storage and analysis periodically.

Figure 2

Another example of M2M interactions that may take place in this healthcare solution model is the interaction between the health monitoring company system and the electronic lock that is on John's front door. For medical personnel to enter his home when they arrive, the health monitoring company system sends a one-time-use code to the lock, shown in Figure 2.

If you'd like to to learn more about connected transportation visist the Cisco FOCUS website.

5.1.3 M2P interactions

In the healthcare solution model, a simple M2P interaction involves the equipment used to monitor John. When John's glucose is too low or too high, and he begins to show symptoms, his health can be compromised very quickly. Without treatment, he will quickly become unable to treat himself, and will need medical attention immediately. The health monitoring company system sends an alert to John's devices which he must acknowledge. If John fails to contact the health monitoring company, medical personnel will be dispatched to his location. This M2P interaction helps to prevent John from entering a diabetic coma.

These are some additional examples of where M2P interactions in the healthcare solution model help to improve healthcare for patients:

- The health monitoring company system sends a one-time-use code to a tablet carried by personnel on the mobile patient treatment center so that they can enter John’s house easily when they arrive.
- The health monitoring company collects all of John’s glucose monitor data so that he can see his levels, allowing him to administer the proper amount of insulin.

5.1.4 P2P interactions

These are some of the P2P interactions that take place in the healthcare solution model:

- **Patient to health monitoring company personnel** – When alerted, John must call and speak with a healthcare worker at the health monitoring company. Without this important P2P step, emergency personnel will be dispatched to treat John immediately.
- **Patient to mobile patient treatment center personnel** – When emergency personnel arrive, they will administer medical attention to restore John’s glucose levels to normal. This critical P2P interaction could save John’s life.
- **Doctor to patient** – John must consult with his doctor on a regular basis to ensure that he is following directions to maintain a healthy lifestyle. His doctor may decide to adjust John’s treatment strategy based on this P2P interaction.

5.1.5 Analytical tools

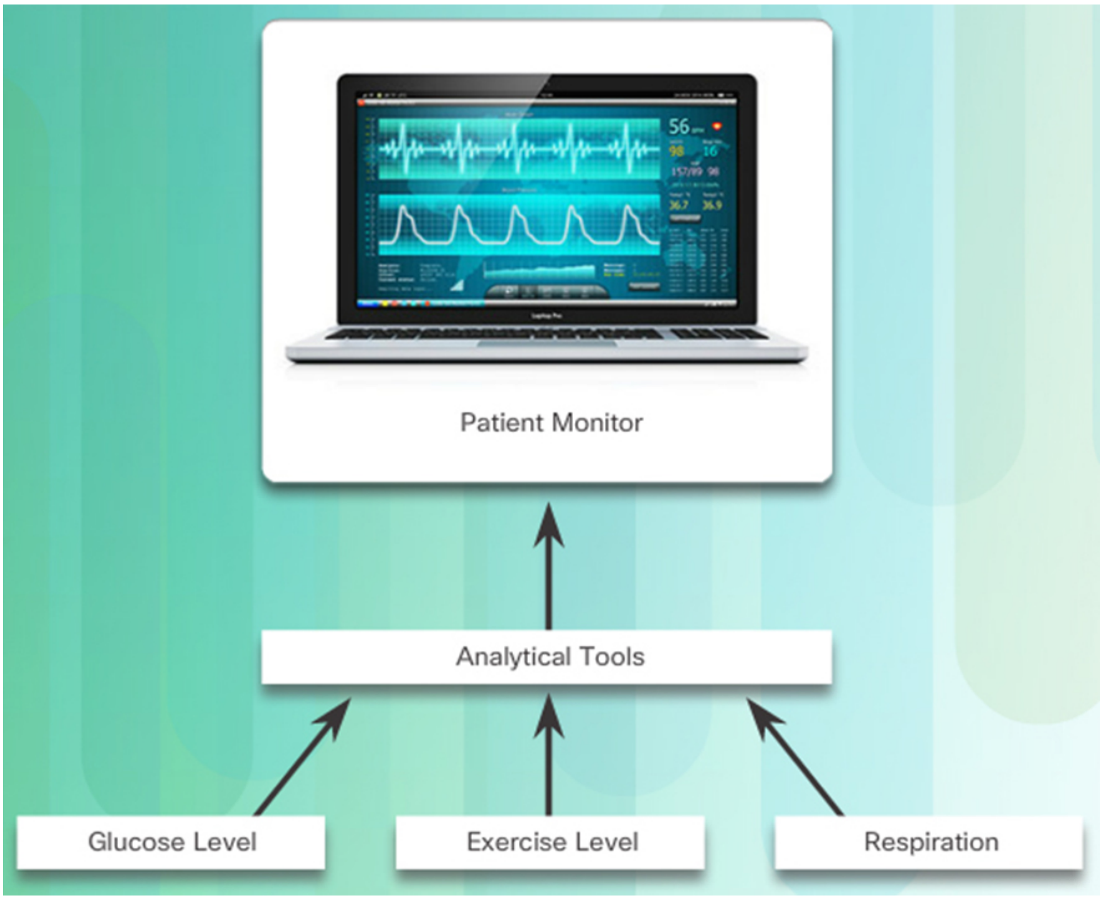


Figure 3

There are enormous amounts of data created in the IoE. To apply this data to processes, people use analytical software. Analytical software ranges from simple spreadsheet tools to determine statistics for a given range of data, to sophisticated business software suites. The software may be created and sold by a large organisation, developed independently and provided through open source means, or designed by the business that uses it for a specific purpose.

The majority of analytics were used as a method of forecasting supply, based on the number of units sold in a given amount of time. Analytics in the IoE has advanced to address many new aspects of business. Some of the following types of analytics are used to help shape how a business functions:

- **Descriptive** – uses historical data to create reports designed to facilitate understanding.
- **Predictive** - uses data mining and modeling techniques to determine what could happen next.
- **Prescriptive** – uses simulation, business rules, and machine learning to recommend a course of action and what the outcome of that action might be.

In the healthcare solution model, the health monitoring company uses analytics of all kinds to improve the quality of healthcare.

5.1.6 Analytics in healthcare

In the healthcare solution model, IoE technology improves healthcare by analysing trends in a patient's vital signs and other indicators such as blood glucose levels. This data can be monitored in real-time to alert the patient and the health monitoring company so that they can make decisions quickly and correctly. As a patient goes about daily life, data is constantly gathered by sensors worn by the patient. This data is sent back to the health monitoring company for storage and analysis. Over time, this data is analysed to find trends which are used to determine if the patient may require immediate assistance.

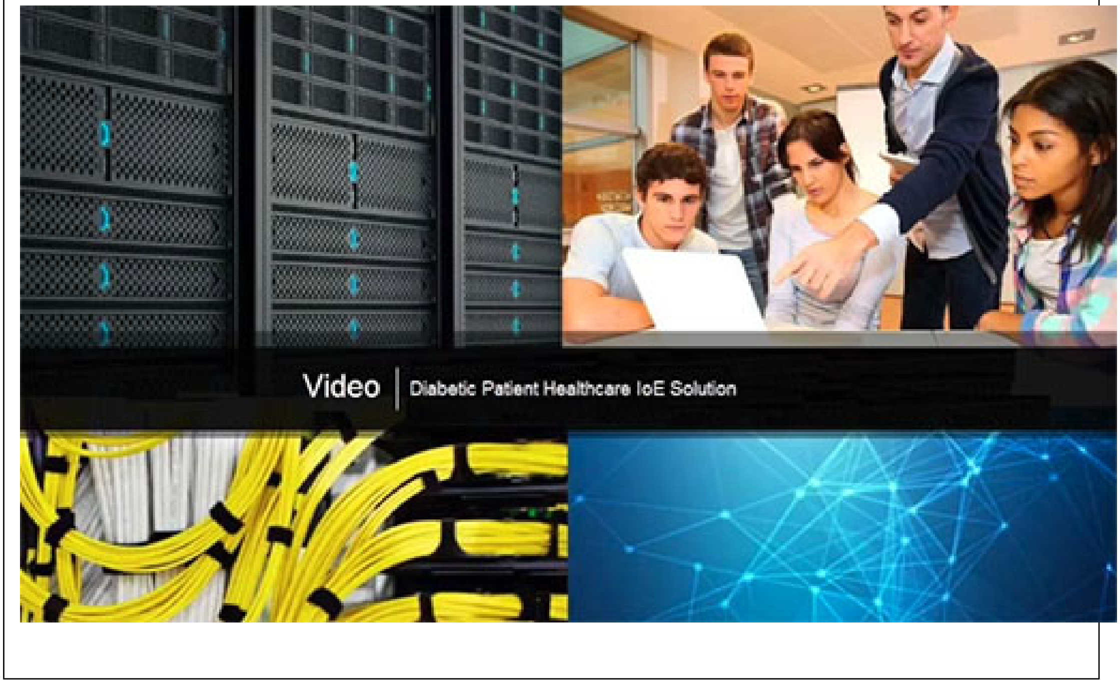
IoE technology in this healthcare solution model is not used just for monitoring a patient's health. It is also used in many other areas to improve healthcare. For example, data from live traffic cameras and historical traffic data can be used to route the mobile patient treatment center more effectively to arrive at a patient's location faster. New uses for IoE technology in the healthcare industry are being discovered every day to help patients live longer, healthier lives.

5.1.7 Packet tracer: diabetic patient healthcare IoE solution

This packet tracer activity simulates an IoE Healthcare solution for a fictitious person, John Doe.

Watch a demonstration of the Packet Tracer activity.

Video content is not available in this format.



The video demonstration is the primary source for how to navigate the activity. However, after viewing the video, you can click the following files to investigate the activity on your own.

- Packet Tracer – Diabetic Patient Healthcare IoE Solution.pdf
- Packet Tracer – Diabetic Patient Healthcare IoE Solution.pkz

Essential note: If you are new to Packet Tracer, you can watch a tutorial. You must install Packet Tracer before you can open .pkz files. To install Packet Tracer, return to the course progress page where a copy is available to download and install .

Packet Tracer is available for both Microsoft Windows and Linux systems. The Open University Cisco Academy team support a moderated Facebook Community helping Mac users port this application onto all versions of the Apple Mac OSX. For more information, you will need to join the community.

5.1.8 Value in good modelling

As you learned in the packet tracer activity, modelling is a valuable step in the implementation of an IoE solution. By modelling the potential solution, the changes in the organisation’s processes are visualised. The model can be shared among all stakeholders to ensure an understanding of how the new solutions work and interact.

A model can be a representation of a system. Models help individuals and organisations better understand the processes that are implemented and help identify problem areas. Models help to run 'what if' scenarios that reveal the benefits and impediments to implementing a new solution. When an organisation begins process re-engineering, it is beneficial to use modeling prior to executing any plans.

While modeling may not be easy, the benefits of good modeling outweigh the costs of poor or rushed modeling for most organisations.

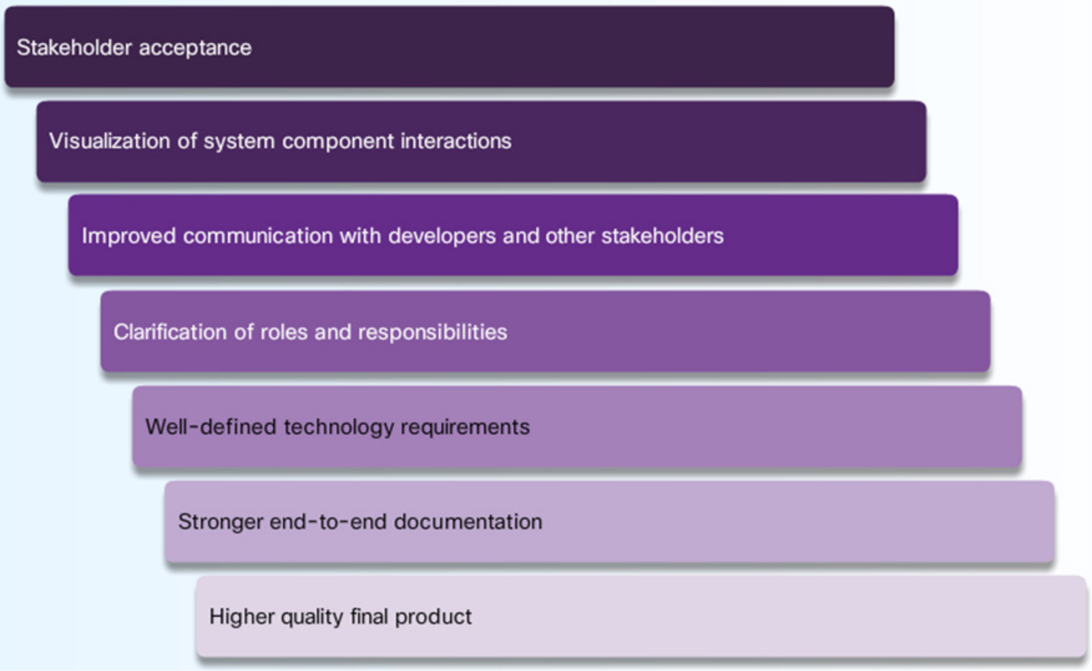
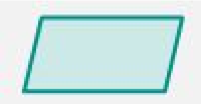
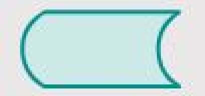
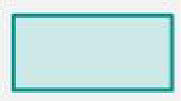
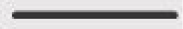

Stakeholder acceptance
Visualization of system component interactions
Improved communication with developers and other stakeholders
Clarification of roles and responsibilities
Well-defined technology requirements
Stronger end-to-end documentation
Higher quality final product

Figure 4

5.1.9 Flowcharts

Organisations can begin to identify the processes that may require re-engineering by using a flowchart. Flowcharts are graphical representations of the workflows that businesses use to analyse and document existing systems, as well as design and manage process re-engineering efforts. A flowchart uses symbols to represent workflows and decisions.

Table 1 Flowchart key

Symbol	Name	Description
	Data	This symbol represents data. It is not intended to be specific as to the type of medium for the data
	Stored data	This symbol represents stored data, which is intended as data that is ready for processing. It is not intended to be specific as to the type medium for the stored data
	Process	This symbol represents a processing function. For example, it may indicate a single, defined operation that changes the value of information. Alternatively, it may indicate a group of operations that change the value or form of information. It may also represent the determination of one of several directions to be followed in a flow
	Line	This symbol represents the flow of data or control. It may include solid or open arrowheads to indicate direction of flow where necessary or to enhance the readability.

The basic symbols for a flowchart, as described by the International Organisation for Standardisation (ISO) are shown in Table 1. The ISO also describes a number of specific symbols for data and process that are not referenced in the figure.

5.1.10 Healthcare model flowchart

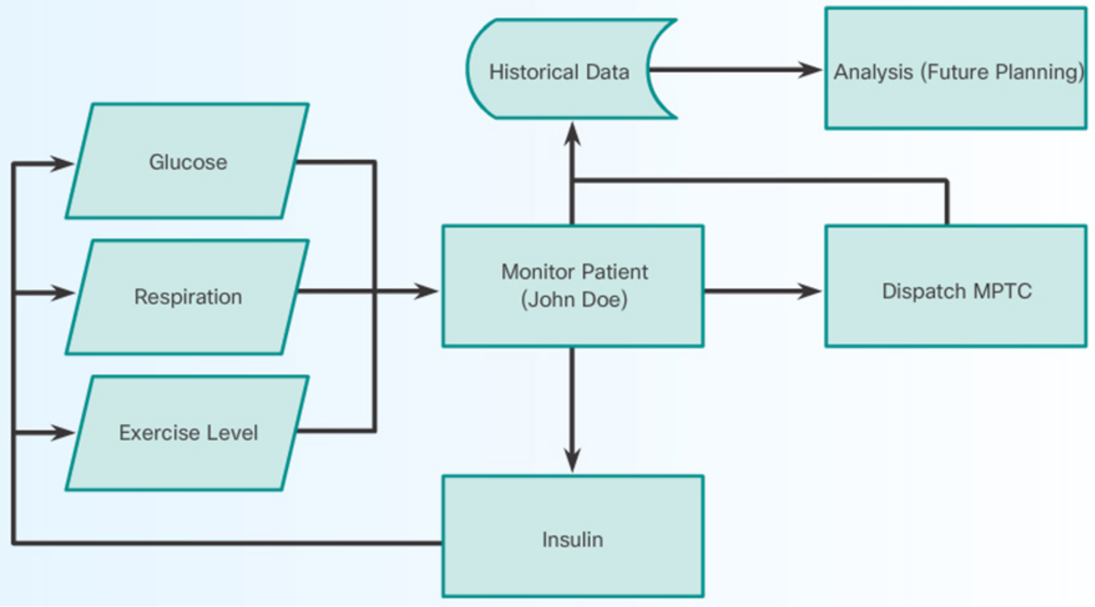


Figure 5

!Warning! CiscoSansTTLight,Helvetica,Arial,sans-serif not supportedThe figure shows a flowchart of basic processes in our model of a healthcare solution. (It uses same the same key as in Table 1). Wearable sensors on a patient provide monitoring to inform patients and other healthcare workers while creating an historical record to identify trends in a patient's health. Based on these trends, a patient may be notified of an unhealthy condition, or medical personnel may be dispatched. This is an example of a feedback loop. Additionally, analysis of historical data can help to identify opportunities and improvements in the overall operation of the healthcare system. This can lead to future processes that help patients in ways we cannot identify now.

5.1.11 Physical topology

A network topology is a kind of map that identifies various elements of a computer network. A network is represented by two topology types: physical and logical.

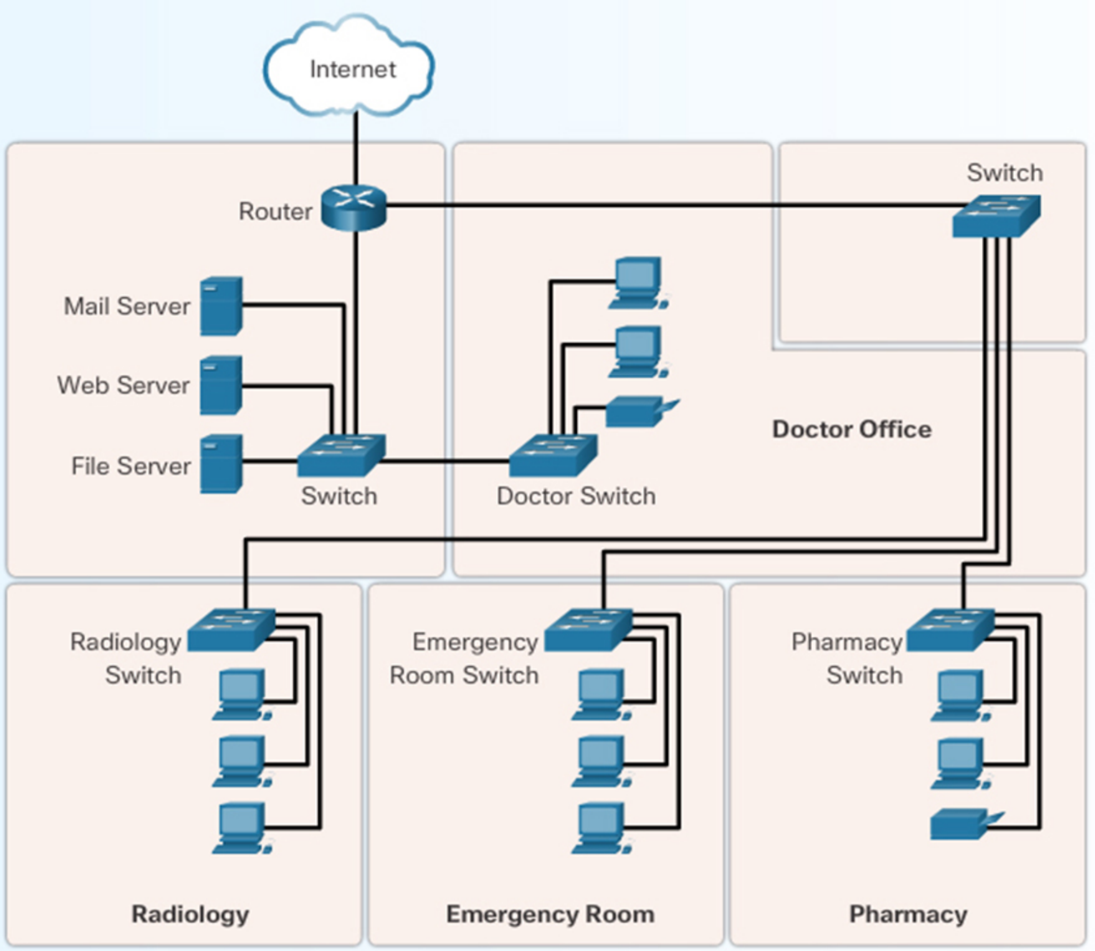


Figure 6 Physical topology

The physical topology displays the layout and location of all of the devices that comprise the network. The physical topology describes how devices are actually interconnected with wires and cables, as shown in Figure 6.

This physical topology will change when mobile devices are incorporated into the network. Mobile devices require connectivity, regardless of their location, for access, monitoring, and control. Some sensors may be located beyond the range of traditional wireless solutions and it may be too expensive to connect them with data cabling. Cellular connections may be required to provide the necessary data links to controllers, central data storage or processing equipment.

The mobile devices must be represented in the physical topology. For wireless connectivity, an inspection, called a site survey, should be done to determine a basic, physical topology.

These are some considerations when determining a physical topology:

- the location of user computers
- the position of network equipment, such as switches, routers, and wireless access points
- the position of controllers and servers
- the position of sensors and actuators
- the potential for future network growth.

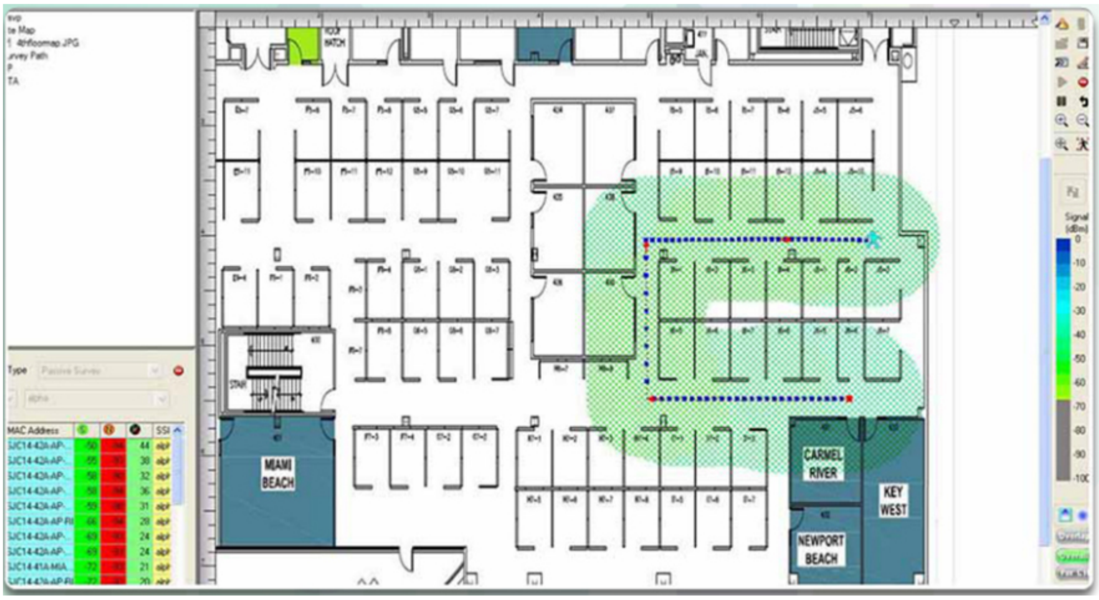


Figure 7 Wireless site survey

Wireless access points must be strategically placed throughout the hospital to relay data. A wireless survey shows where the wireless access points can be located and the strength of the wireless signals, as shown in Figure 8. Wireless access points may be moved to distribute coverage, or additional access points may be installed where needed. The physical topology must be updated to reflect any devices that have been relocated or added.

5.1.12 Logical topology

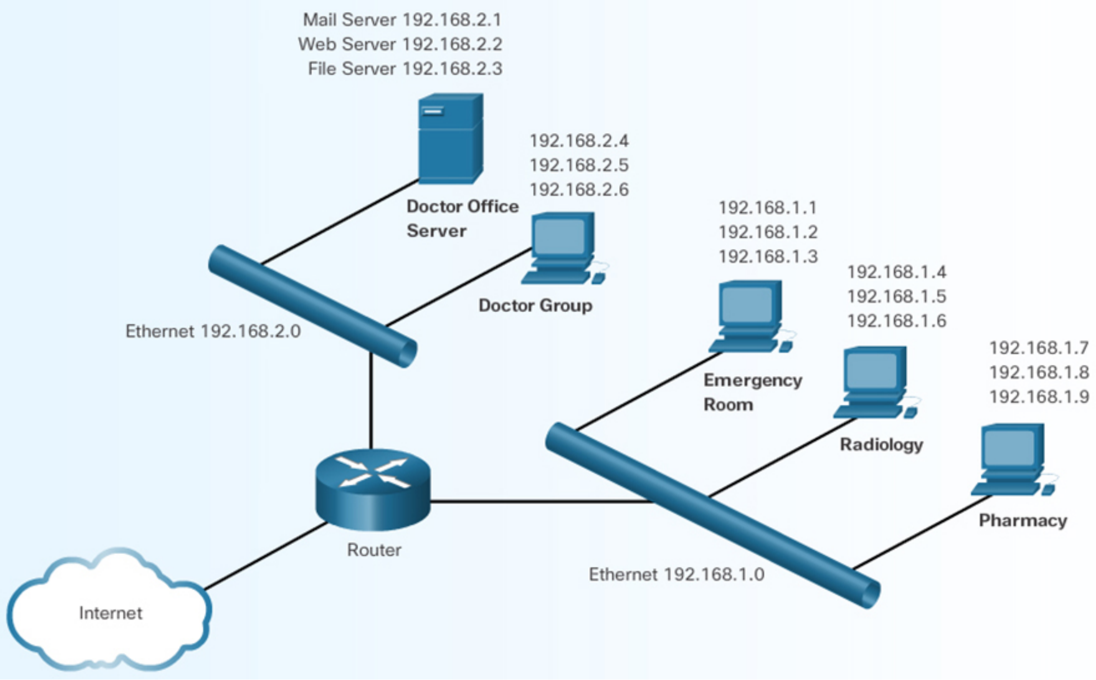


Figure 8

Logical topologies are based on how the communication protocols work and convey a different perspective than physical topologies. The logical topology represents the way data flows through the network. It describes how devices exchange data with network users. As shown in the figure, an integral part of the logical topology is the addressing scheme. This addressing scheme helps identify network and data needs.

After modelling the solution, the next step is to build a prototype.

5.2 Prototyping your ideas

Prototyping is the act of trying out your ideas on a system before it goes into live use. Prototypes do not need to be perfect, their purpose is to help you explore if an idea will work and give you the opportunity to refine it into a working ‘production ready’ system.

In this section you will explore how prototyping helps in the development of IoE systems.

5.2.1 Defining prototyping

Following are some phrases that define a prototype:

- fully functional, but not fault-proof
- an actual working version of the product
- used for performance evaluation and further improvement of product
- has a complerte interior and exterior
- may be relatively expensive to produce
- in the IoE, often used as a technology demonstrator.

Prototyping is the next step in modelling. For the prototyping in the IoE, it helps to have design skills, electrical skills, physical/mechanical skills (working 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 IoE is still developing, there are still unknown tasks to discover. This is a great time to invent something that is part of the IoE. Because the IoE combines people, process, data, and things, there is no end to the inventions that the IoE can help create and then incorporate.

For news and ideas that are already being talked about in the IoE, visit the Cisco IoE Newsroom.

5.2.2 How to prototype and further resources

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. If you like you can watch a TedTalk about this process.

Of course, Google has a large amount 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. The Pebble Watch Kickstarter video was used to generate donations to help this group of inventors create the Pebble Watch.

What IoE invention will you create?

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 the Makezine website.

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. Making Society has a good section on modeling plastic and clay. You might be surprised with what you can do with plastic, clay, paper, and wires. For more information or ideas, go to the Making society website.

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.

Meccano 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.

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. An example is Makerbot.

Electronics toolkits

Computer programs cannot run without a computer. While you can create programs for almost any computer, some platforms are designed for the beginner. Following 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.

While Arduino is not suitable for use as a computer, the 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.

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.

Programming resources

Programming is critical to the IoE. Creating custom code is very useful when developing an IoE solution. You have already learned about Scratch. There are many other free resources that can help you get started with programming.

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

Khan Academy is a non-profit educational website created in 2006 to provide 'a free, world-class education for anyone, anywhere'. There are lectures related to computer programming.

Code Academy is another excellent resource. It relies on interactivity to help people learn how to write computer programs.

There are also aa number of coures on OpenLearn including *Learn code for data analysis*.

Community inventor and entrepeneurship

So, perhaps you have just created something really neat. What now? There are a number of places where you can get help exposing your idea or prototype to others.

Investigate what is available in your community. Check with your local government, schools, and chamber of commerce for information about workshops, classes, and expert advice.

The internet has many resources to help your idea get exposure. A good example is Quirky. Quirky allows users to share their ideas. When an idea is submitted, other Quirky users can vote and choose whether or not they want to support your idea. If an idea is good, it may become a real product.

If you do not want to share your idea and all you want is information, Ask the Inventors is a great resource. Their website provides detailed information on all the phases of your project.

5.3 Want to go further?

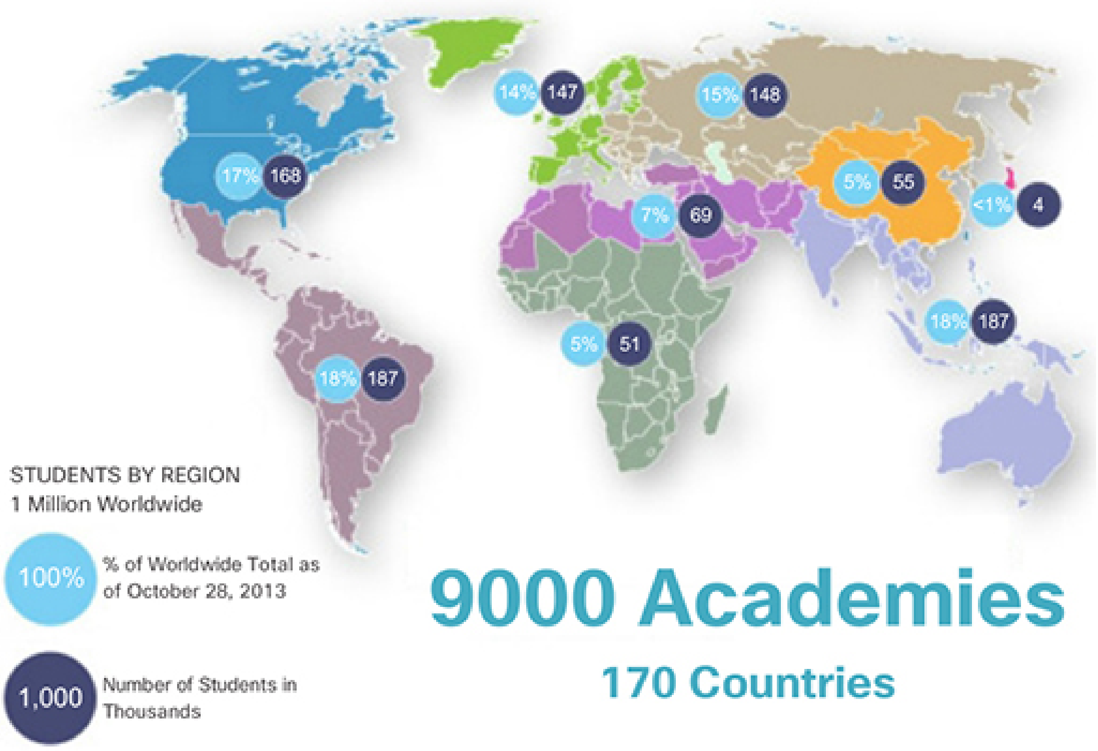


Figure 9

The rapid growth of networks has created a global shortage of people who are qualified to implement and maintain networking solutions, especially in places where networks are being built to promote economic development. At the same time, people need access to better training and career opportunities to successfully compete in the global economy.

With 9,000 academies in 170 countries, the Cisco Networking Academy helps individuals prepare for industry-recognised certifications and entry-level information and communication technology (ICT) careers in virtually every type of industry. The Cisco Networking Academy helps address the growing demand for ICT professionals, while improving career prospects in communities around the world.

Cisco Networking Academy has trained more than four million students to date. Many graduates have gone on to successful ICT careers in a variety of industries, while others have harnessed the entrepreneurial spirit and knowledge they acquired to start their own businesses and create new jobs.

5.3.1 Networking Academy curricula

The Networking Academy delivers a comprehensive, 21st century learning experience. Students develop the foundational ICT skills needed to design, build, and manage networks, along with career skills such as problem solving, collaboration, and critical thinking. Students complete hands-on learning activities and network simulations to develop practical skills that will help them fill a growing need for networking professionals around the world. These are some of the offerings of the Networking Academy:

- **IT Essentials** − IT Essentials covers the fundamentals of computer hardware and software and advanced concepts, such as security, networking, and the responsibilities of an IT professional.
- **Entrepreneurship** − The Entrepreneurship course teaches critical business and financial skills, attitudes, and behaviors to help students develop an entrepreneurial mindset that can empower them to improve their overall quality of life.
- **Introduction to Cybersecurity** − The Introduction to Cybersecurity course covers trends in cybersecurity and demonstrates the need for cybersecurity skills in various industries.
- **CCNA Routing and Switching** − CCNA Routing and Switching provides a comprehensive overview of networking concepts and skills. It covers network applications to the protocols and services provided to those applications by the lower layers of the network. This curriculum has an emphasis on practical application, work-force readiness, and soft-skills development.
- **CCNA Security** − CCNA Security introduces the core security concepts and skills needed to install, troubleshoot, and monitor a network to maintain the integrity, confidentiality, and availability of data and devices.

For more information on our latest offerings, go to the Networking Academy website.

5.3.2 IT industry certifications

Industry certifications are highly respected by employers around the world and help validate the skills needed to launch successful careers in networking and ICT. Certifications are achieved by passing an exam proctored by a certifying authority. Students must complete training materials specific to the certification exam. Field experience is often very helpful, but not always required, to pass a certification exam. Cisco Networking Academy provides courses that prepare students for the industry certifications that are shown in Table 2.

Table 2 Cisco Networking Academy courses

CompTIA A+	CCENT	CCNA Routing and Switching	CCNA Security
The CompTIA A+ certification for computer support technicians demonstrates competence in areas such as installation, preventive maintenance, networking, security, and troubleshooting. IT technician, IT administrator, and field service technician are examples of jobs that students can pursue	The Cisco CCENT certification for entry network technicians validates the ability to install, operate, and troubleshoot a small branch network and perform basic network security tasks. Support desk technician and network support technician are examples of jobs that students can pursue using the Cisco CCENT certification.	The Cisco CCNA Routing and Switching certification validates the ability to install, configure, operate, and troubleshoot medium-sized routed and switched networks, and implement and verify connections to remote sites in a wide-area network (WAN). Examples of jobs that the CCNA Routing and Switching certification can help students to find are	The Cisco CCNA Security certification for network security professionals validates the knowledge needed to install, troubleshoot, and monitor Cisco network security devices; develop a security infrastructure; recognise network vulnerabilities; and mitigate security threats. Students who gain CCNA Security certification would be well qualified for a

using the CompTIA A + certification.	network administrator, network installer, and network engineer.	position as a network security specialist.

There are two basic types of certification available: vendor-specific and vendor neutral. Vendor-specific certifications are tailored to technologies offered by a company to prove that an individual is qualified to deploy and manage that technology. Vendor-neutral certifications are offered by many different organisations. They show that an individual has a well-rounded skillset centered on common systems and programs, rather than specific types of technology.

Most often, certifications must be renewed over time. Requirements for re-certification may be earning continuing education units (CEUs), passing a re-certification exam, or both. CEUs can be earned by attending classes, professional membership, on-the-job experience, or research and publishing of materials that support the certification technology.

Table 3 Cisco certification tracks

Certification tracks	Entry	Associate	Professional	Expert	Architect
Collaboration				CCIE Collaboration	
Data Center		CCNA Data Center	CCNP Data Center	CCIE Data Center	
Design	CCENT	CCDA	CCDP	CCDE	CCAr
Routing & Switching	CCENT	CCNA Routing and Switching	CCNP	CCIE Routing & Switching	
Security	CCENT	CCNA Security	CCNP Security	CCIE Security	
Service Provide		CCNA Service Provider	CCNP Service Provider	CCIE Service Provider	
Service Provider Operations	CCENT	CCNA Service Provider Operations	CCNP Service Provider Operations	CCIE Service Provider Operations	
Video		CCNA Video			
Voice	CCENT	CCNA Voice	CCNP Voice		
Wireless	CCENT	CCNA Wireless	CCNP Wireless	CCIE Wireless	

The Cisco Certification Tracks are shown in Table 3. To explore all of the different Cisco career certifications, visit the Cisco Learning Network website.

5.3.3 Additional learning opportunities

Certifications can show an employer that an individual has the appropriate skills for a job. University degrees can show that a person has gained a broad understanding in an educational field. This broad understanding creates a solid foundation for emerging career opportunities in the IoE. A combination of industry certifications and university degrees provides a student with the best background, experience, and education to pursue a career with greater opportunities and higher salary.

When looking for a degree to pursue at a college or university that will pertain to the skillsets needed for a career in the IoE, look out for some of the following degrees:

- Business Intelligence
- Computer Information Systems
- Computer Programming
- Computer Science
- Database Administration
- Electromechanical Automation
- Electronics Engineering
- Linux Networking
- Machining
- Network Administration
- System Analysis
- Web Server Administrator

This is not an exhaustive list. Even traditional degree programs such as supply chain management, business, and project management are helpful for careers in IoE. Computer-aided design (CAD), drafting, math, and physics are applicable and show a diverse education, which is perfect for an IoE career.

The Open University is part of the Cisco Networking Academy programme. You can find out more about our Cisco courses and also explore our full computing prospectus.

5.3.4 IT industry jobs for the IoE

IoE is creating demand for a broad spectrum of IT jobs. These opportunities may be specific to Fog computing, developing new processes, or a specialisation in a discipline that has not yet been realised. These jobs reflect skills spanning multiple disciplines that include computer science, computer engineering (a blend of computer science and electrical engineering), and software engineering in the following areas:

- collaboration
- enterprise networks
- data centre and virtualisation.

Create your own IoE job

IoE is also creating demand for a new kind of IT specialist, individuals with the skillsets to create new products and process the data they collect. A workforce is needed that specialises in both information science and software or computer engineering.

Additionally, operational technologies and information technologies are converging in the IoE. With this convergence, people must collaborate and learn from each other to understand the things, the networks, and methodologies to harness the limitless potential of the IoE.

5.4 Terms and concepts practice

This activity will help you to test some of the terms and concepts you've been introduced to.

model

physical topology

logical topology

predictive analytics

prototype

M2M interaction

M2P interaction

flowchart

Match each of the items above to an item below.

a representation of a system

a kind of map of the layout and location of all of the devices that comprise a network

a diagram illustrating the flow of data through a network

uses data mining and modelling techniques to determine what will happen in the future

a fully functional working version of a product that is under design

a sensor sends data to a controller which activates an actuator

a sensor sends data to a controller which sends an alert to a gateway which pages an employee

uses symbols to represent workflows and decisions

5.5 Session 5 quiz

Check what you have learned in Session 5.

Session 5 quiz

Use 'ctrl' (cmd on a Mac) or right-click to open the quiz in a new window or tab then come back here when you're finished.

5.6 Summary

The healthcare model that is used in this chapter details M2M, M2P, and P2P interactions. It models every aspect of patient monitoring from basic vital signs to dispatching healthcare professionals to treat patients.

Descriptive, predictive, and prescriptive analytics help shape how a business functions.

Modelling the potential IoE solution identifies the changes in the organisation’s processes. organisations identify the areas that are best served by re-engineering processes using a flowchart. A flowchart uses symbols to represent workflows and decisions.

A network topology is a kind of map. There are two types of network topologies, physical and logical. The physical topology displays the layout and location of all of the devices that comprise the network. The logical topology represents the way data flows through the network.

To prototype ideas for the IoE, 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.

Programming is critical to the IoE. There are many other free resources that can help you get started with programming. Three of the most popular platforms are Arduino, Raspberry PI, and Beaglebone. Check with your local government, schools, and chamber of commerce for information about workshops, classes, and expert advice.

The Cisco Networking Academy helps individuals prepare for industry-recognised certifications and entry-level information and communication technology (ICT) careers in virtually every type of industry. The internet of everything is creating demand for a broad spectrum of IT jobs, and creating opportunities for exciting new jobs in emerging fields.

You've nearly finished! The next section takes you to the final assessment quiz.

5.7 Final assessment quiz

To complete the course and gain your free statement of participation, take the final assessment quiz:

Final assessment quiz

Once you've completed it you've finished the course. Congratulations! You should receive notification that your free Statement of Participation is ready within 24 hours.

Now you've completed the course we would again appreciate a few minutes of your time to tell us a bit about your experience of studying it and what you plan to do next. We will use this information to provide better online experiences for all our learners and to share our findings with others. If you'd like to help, please fill in this optional survey.

References

Session 1

TeleGeography (n.d.) 'Submarine cable map' [Online]. Available at http://www.submarinecablemap.com/ Accessed 12 July 2016.

Acknowledgements

The *Internet of everything* free course is brought to you by The Open University. This course was originally developed by Cisco Systems Ltd and adapted for OpenLearn by The Open University. The collaboration of The Open University and Cisco Systems to develop and deliver this course as part of OpenLearn's portfolio will provide and extend free learning in this important and current area of study.

The material acknowledged below is Proprietary and used under licence (not subject to Creative Commons Licence). Grateful acknowledgement is made to the following sources for permission to reproduce material in this course:

Videos: © Cisco Systems http://www.cisco.com/
https://creativecommons.org/licenses/by-nc-nd/4.0/

Every effort has been made to contact copyright owners. If any have been inadvertently overlooked, the publishers will be pleased to make the necessary arrangements at the first opportunity.