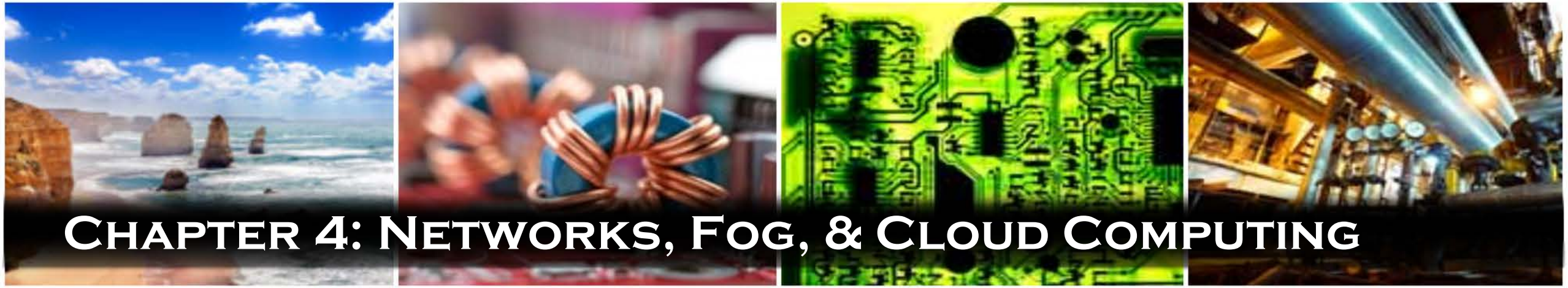
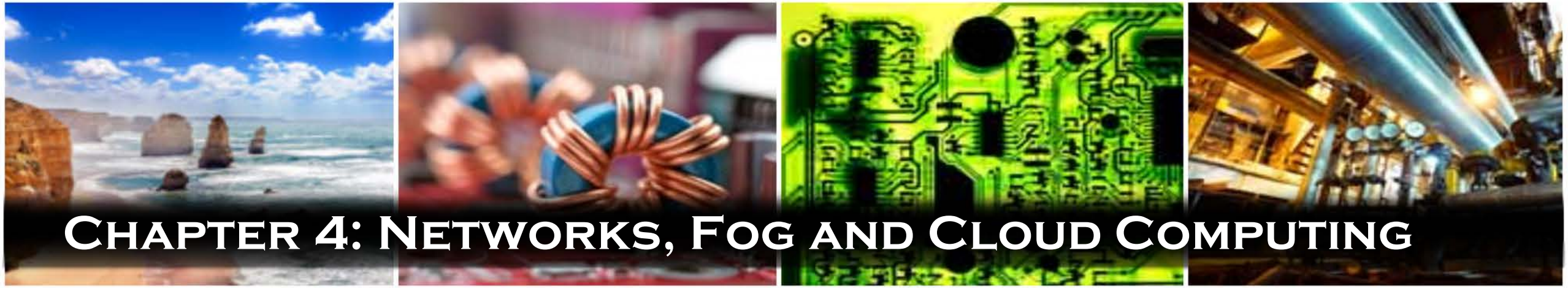


Chapter 4: Networks, Fog, & Cloud Computing

IoT Fundamentals
Connecting Things 2.0
Instructor Training

Education Service Center Region 11
Academy Support/Instructor Training Center

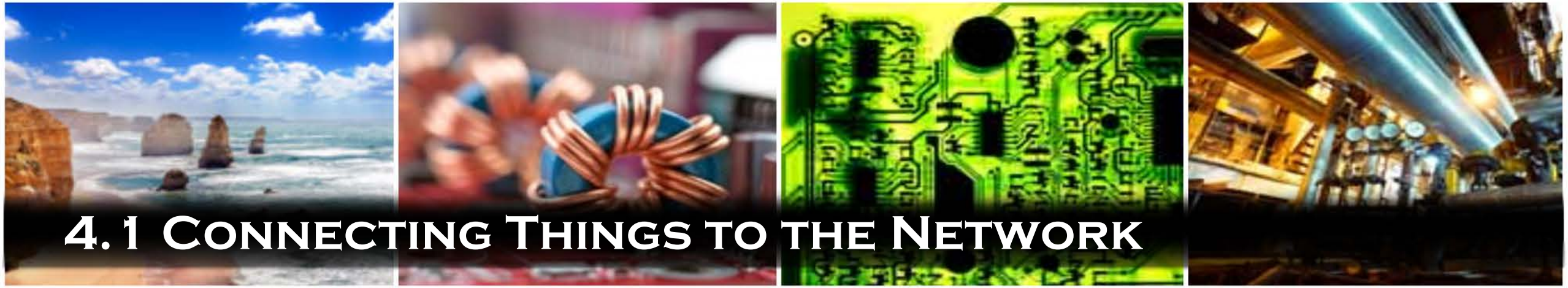


Chapter 4: Networks, Fog and Cloud Computing

IoT Fundamentals
Connecting Things 2.0

Chapter 4 - Sections & Objectives

- 4.1 Connecting Things to the Network
  - Explain how the network supports the IoT
- 4.2 Fog and Cloud Computing
  - Explain why fog and cloud computing are used in IoT systems

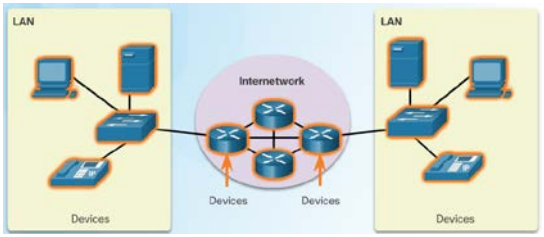


4.1 Connecting Things to the Network

Education Service Center Region 11
Academy Support/Instructor Training Center

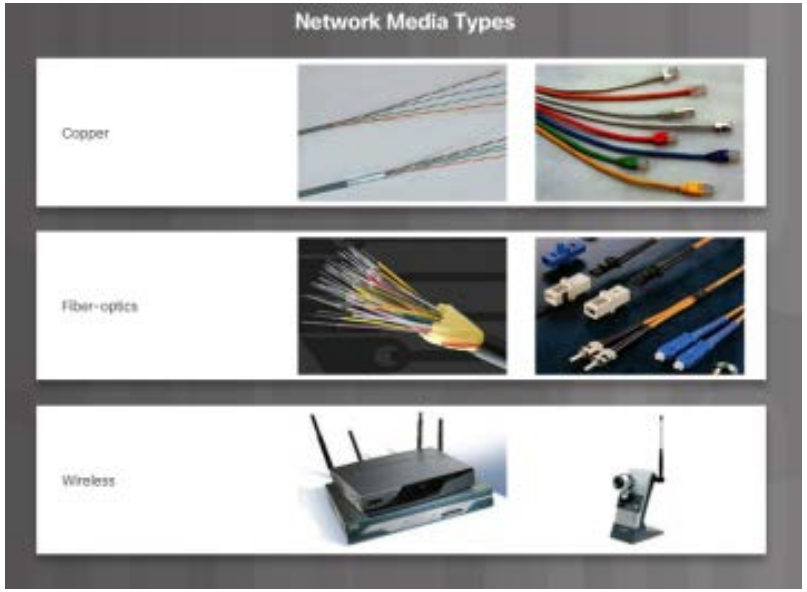
4.1.1 The Role of the Network

- **LAN and WAN**
  - The path from source to destination can be a single cable or a collection of networks
  - A **Personal Area Network (PAN)** is a type of network that usually spans a few meters around an individual and is often used in IoT
  - A **Local Area Network (LAN)** is a type of network infrastructure that spans a small/limited geographical area and is used to connect end devices
  - A LAN is normally a high-speed network under the control of a single administrative entity
  - A **Wide Area Network (WAN)** is a type of network infrastructure that spans a wide geographical area and is used to connect WANs
  - A wide area network is usually administered by multiple service
  - A WAN is normally a low-speed network and may include portions administered by multiply Internet Service Providers (ISPs)
  - LANs often connect machines in the factory plant
  - WAN devices have evolved to create **Low-Power Wide Area Networks (LPWAN)** for use in the IOT



4.1.1 The Role of the Network

- **Network Devices and Communication Media**
  - Network devices are devices that connect to each other through a network
  - An end device is either the source or destination of a message transmitted over the network
  - Intermediary devices connect the individual end devices to the network and can connect multiple individual networks to form an internetwork
  - Network addresses are used to uniquely identify devices on a network
  - Network media provide the physical channel over which the message travels from source to destination
  - Types of media:
    - Copper wires uses electrical impulses
    - Fiber optic cable uses pulses of light
    - Wireless uses radio waves

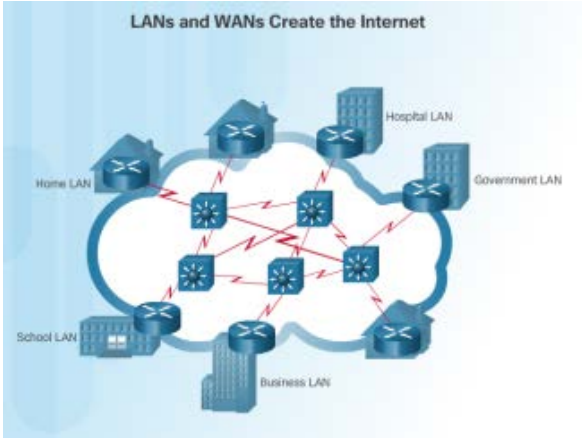


4.1.1 The Role of the Network

- **Parts of the IoT:**
  - End devices - source or destination of a message
  - Intermediate devices - determine best path for packets
  - Media - physical channel to carry messages
  - Services - network applications

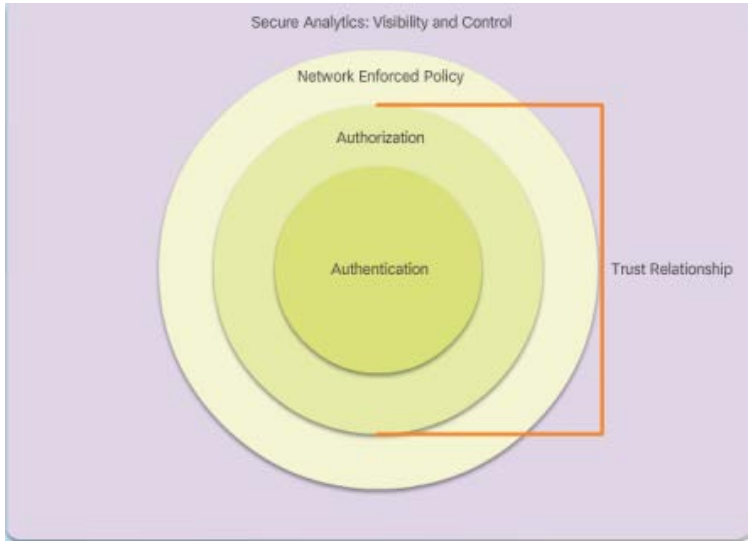
4.1.1 The Role of the Network

- **Network Protocols**
  - **Protocols** are rules governing communication between network devices
  - Devices must conform to common protocols before they can communicate
  - Two very important network protocols are Ethernet and IP
  - Ethernet rules enable communication between local devices
  - IP enable communication between remote devices
- **Basic Routing**
  - The role of routing on data networks is to determine the best paths for packets through the network
  - Network packets must often transverse several networks to get to the destination
  - Routing is the process of directing a network packet to its destination
  - Routers are intermediary network devices that perform routing
- **LANs, WANs, and the Internet**
  - Single router designs are common in SOHO
  - The single router connects SOHO devices to the Internet
  - The single router is the default gateway for all SOHO devices



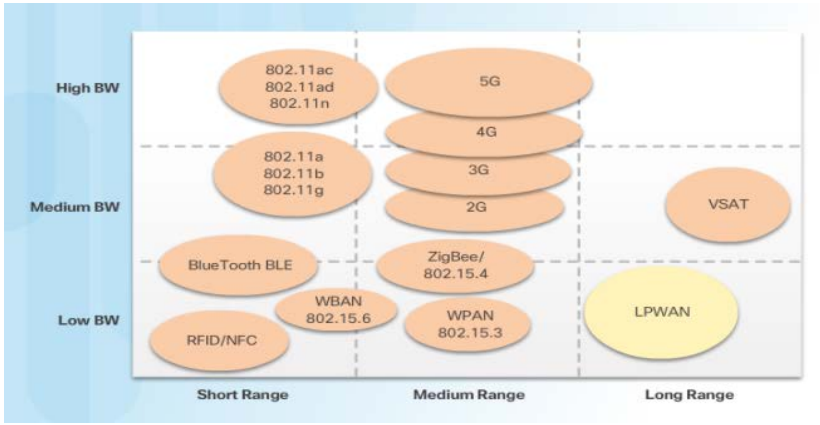
4.1.1 The Role of the Network

- **IoT Protocols**
  - IoT Devices are often embedded devices designed to work in sub-optimal conditions
  - These devices require specialized protocols to function with low power and limited connectivity
  - IoT devices use **CoAP (Constrained Application Protocol)** and **MQTT (Message Queuing Telemetry Transport)**
- **Securing the Network**
  - IoT devices are integrated into all aspects of daily life
  - IoT applications carry traceable signatures and carry confidential data
  - IoT devices must adhere to a secure framework (Authentication, Authorization, Network Enforced Policy, Secure Analytics)



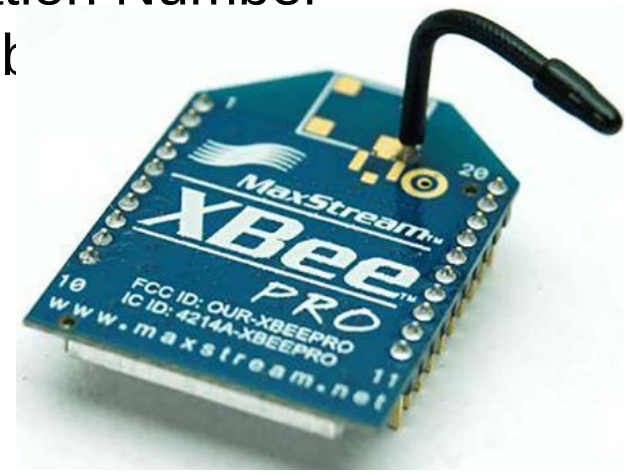
4.1.2 Wireless Technologies

- **Wireless**
  - Wireless connectivity is the biggest growth area
  - New protocols created/updated to support diverse IoT devices:
    - ZigBee - popular in IoT applications such as home automation
    - Bluetooth - used for data communication over short distances
    - 4G/5G - cellular-based technology for transferring data over large geographic areas
    - LoRaWAN - uses a gateway to relay messages between end-devices and a central network server
  - Protocols created for short, medium, and wide ranges
  - **Low-Power Wide-Area Networks (LPWAN)** is designed to support long range communications for low bit rate devices such as sensors, actuators, and controllers
  - WPA and WPA2 are protocols developed by the Wi-Fi Alliance to secure wireless networks



4.1.2 Wireless Technologies

- ZigBee
  - A low-energy, low-power, low-data rate wireless protocol specification used to create personal area networks
  - Areas of utilization:
    - home automation
    - medical device data collection
    - other low-power low-bandwidth needs
  - 250 kbps transfer rate best suited for intermittent data transmissions
  - Every ZigBee data request uses an Application Profile Identification Number
  - Application profile ID numbers - 16-bit numbers that relate to pub manufacturing profiles, or private profiles.
  - ZigBee version 1.2 has a number of serious and exploitable security vulnerabilities
  - Most of these protocol design flaws relate to attempts to make it easier for the end-user to add a ZigBee device to the ZigBee network



4.1.2 Wireless Technologies

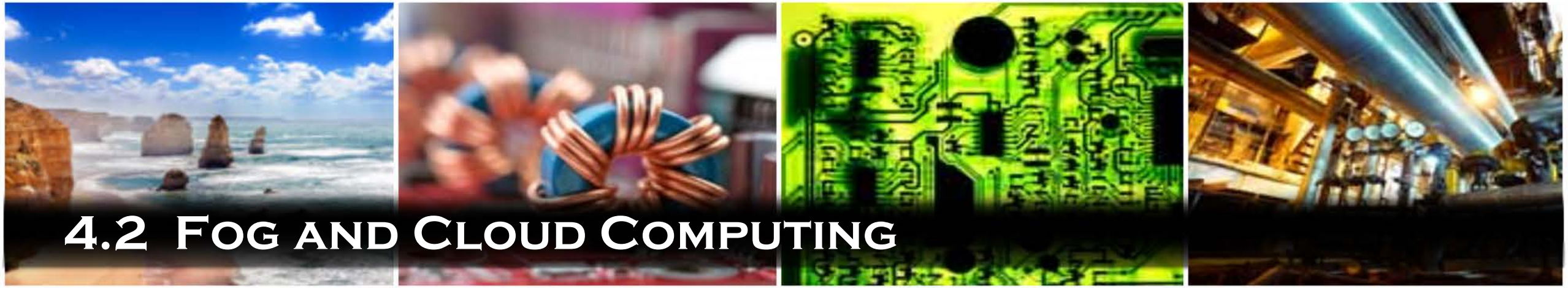
- **Bluetooth**
  - Wireless protocol used for data communication over short distances (PAN)
  - Supported by almost all mobile devices and accessories - the defacto standard for audio between mobile devices
  - Bluetooth Low Energy (BLE) - very popular because of the smartphone industry and new applications in healthcare, fitness, and beacons
    - operates in the 2.4 GHz ISM band
    - Has a very fast connection rate (milliseconds) and a very high data rate (1 Mbps)
    - The BLE device then goes into “sleep mode” until a connection is reestablished - lengthens the battery life for several years
  - Beacons use BLE technology - positioned on buildings, in coffee shops, and on light posts to provide location services

4.1.2 Wireless Technologies

- **4G/5G**
  - Cellular-based data networks designed to take advantage of communications over large geographic areas
  - High mobility bandwidth (trains and cars) of 4G system is 100 Mbps
  - Low mobility (pedestrians and stationary users) of 4G systems is 1 Gbps
  - 4G provides support for voice, IP telephony, mobile Internet access, video calling, gaming services, cloud computing, high-definition mobile TV, and mobile 3D TV
  - **Long Term Evolution (LTE)** and **WiMAX (IEEE 802.16e)** are two popular 4G systems
  - LTE 4G technology release 13e includes the standardization of **NarrowBand IoT (NB-IoT)** – an LPWAN technology
  - Next Generation Mobile Networks Alliance defining the standards and requirements for 5G

4.1.2 Wireless Technologies

- **LoRaWAN**
  - Wireless technology designed to provide wireless WAN connections to power constricted devices
  - targets key requirements of the Internet of Things such as secure bi-directional communication, mobility and localization services
  - Architecture is often an extended star topology in which gateways relay messages between end-devices and a central network server is located in the backend.
  - Data rates range from 0.3 kbps to 50 kbps
  - Security is built into the LoRaWAN standard, implemented in a multi-layer encryption scheme.
    - Unique keys are used in the Application, Network, and Device layers



4.2 Fog and Cloud Computing

4.2.1 Fog and Cloud Services

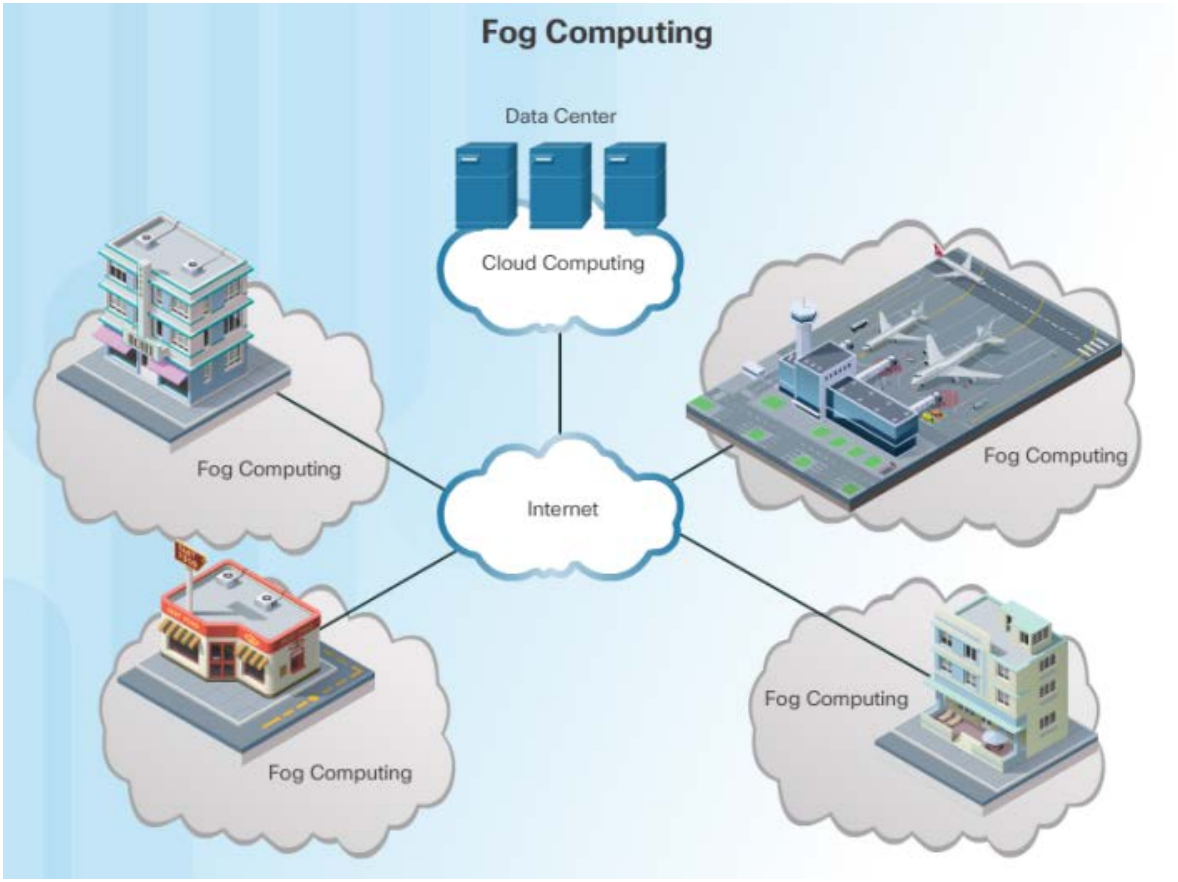
- **Cloud Computing Model**
  - On-demand access to a shared pool of configurable computing resources
  - Resources can be made available quickly with minimal management effort
  - Cloud service providers use data centers for their cloud services and cloud-based resources
  - “Pay-as-you-go” model treats computing and storage expenses as a utility
  - The “pay-as-you-go” payment model is typically used to purchase cloud services
  - Enables access to organizational data and applications anywhere and at any time
  - Reduces cost for equipment, energy, physical plant requirements, and personnel training needs
  - Cloud services offered:
    - Infrastructure as a Service (IaaS)
    - Platform as a Service (PaaS) (mPaaS)
    - Mobile Platform as a Service (mPaaS)
    - Software as a Service (SaaS)

4.2.1 Fog and Cloud Services

- **Cloud Services**
  - Cloud customers have access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort
  - Extends functionality of an IoT system: data processing and storage done in the cloud instead of in the IoT devices
  - Data and resources - always available to any device in the system as long as the device has Internet connectivity
  - Cloud service providers are also very serious about security, ensuring customer data is kept safe and secure
  - Examples of cloud services:
    - Amazon AWS
    - IFTTT
    - Zapier
    - Built.io
    - Cisco Spark
  - **Built.io** cloud service provides an app development platform and a backend service for apps

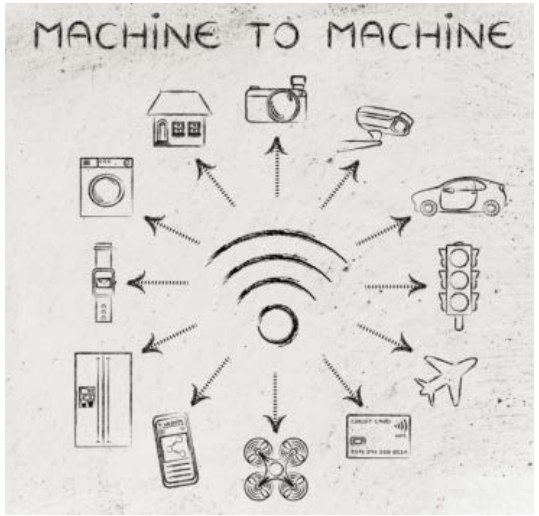
4.2.1 Fog and Cloud Services

- The goal of fog computer is to analyze data as close to the source as possible
- Fog computing allows data to be analyzed and managed at the location where it is generated



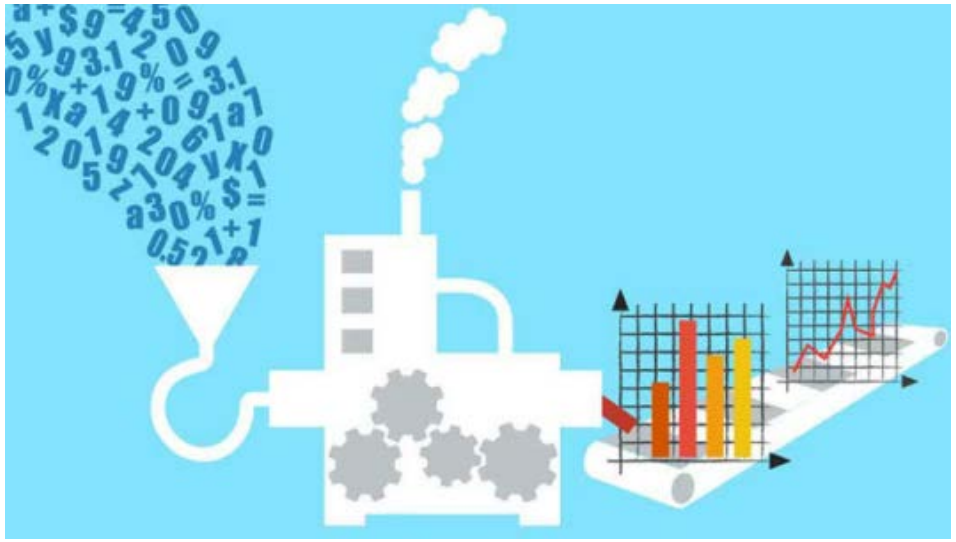
4.2.1 Fog and Cloud Services

- **Fog Computing Model**
  - Distributed computing infrastructure closer to the network edge
  - Edge devices run applications locally and make immediate decisions
  - Reduces the data burden on networks as raw data not sent over network connections
  - Enhances security - keeping sensitive data from being transported beyond the edge where it is needed
  - Fog applications monitor or analyze real-time data from network-connected things and then take action such as locking a door, changing equipment settings, applying the brakes on a train, zooming in with a video camera
  - The action can involve machine-to-machine (M2M) communications and machine-to-people (M2P) interaction
  - Cisco predicts that 40% of IoT-created data will be processed in the fog by 2018



4.2.2 Big Data

- **Data Growth**
  - Number of sensors and other IoT end devices growing exponentially and collecting a constant stream of data
  - Consumer behavior is changing requires anytime, anywhere, on-demand access – fitness monitors, smartphones, medical devices
  - Smart cities and smart grids, connected trains, cars – growing in frequency
  - Problems arise in terms of the requirements for storage, analysis, and security



4.2.2 Big Data

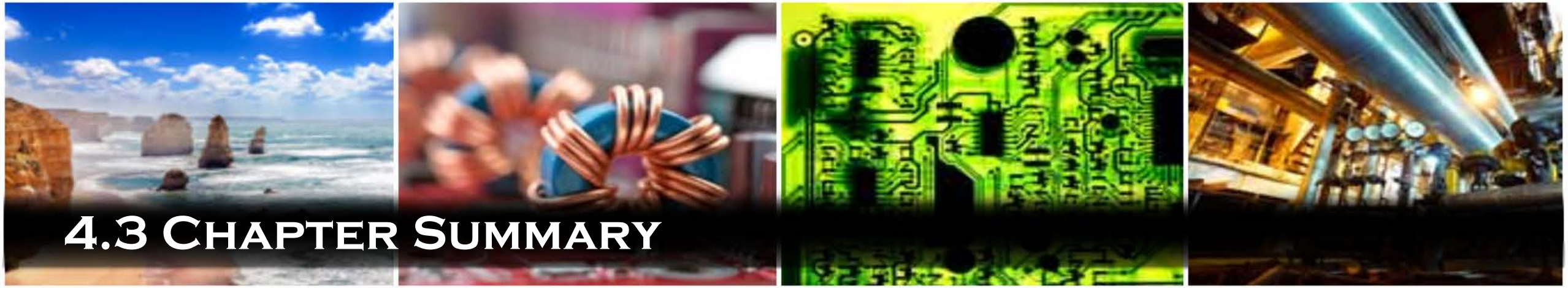
- **All About the Data**
  - Big data is data that is so vast and complex it is difficult to store, process, and analyze using traditional data storage and analytics applications.
  - Characteristics that distinguish big data from data
    - Amount of data being transported and stored
    - Rate at which data is generated
    - Type of data that is generated
  - Typically characterized in three dimensions:
    - **Volume** - the amount of data being transported and stored
    - **Velocity** - the rate at which this data is generated
    - Variety - the type of data, which is rarely in a state that is perfectly ready for processing and analysis
  - Apache Hadoop, Spark, Cassandra, and Kafka – examples of open source projects dealing with Big Data

4.2.3 Security Concerns in the IoT

- **Data Storage**
  - IoT devices may store data for a period of time before sending it out for processing, especially for devices that do not maintain constant connections to their gateways or controllers
  - Critical that all IoT storage devices encrypt data for storage to avoid data tampering or theft
  - Self-encrypting drives have encryption capability built into the drive controller - encryption and decryption done by the drive itself, independent of the operating system
  - Self-encrypting flash memory – manufacturers beginning to release new devices with self-encrypting flash memory

4.2.3 Security Concerns in the IoT

- **Data Transmission**
  - If data is not properly secured through encryption, it can be intercepted, captured or manipulated while in transit
  - Modern encryption algorithms may require more processing power than what is available in the IoT device
  - As well as physical security, IoT devices must be able to protect its own firmware and the data it transmits
  - Ensure that IoT devices are running the latest version of their firmware and protocols
  - Common attack: trick devices into using sub-optimal security parameters under which the connection can be exploited
  - Servers, cloud endpoints, intermediary devices should also be secured and use strong encryption algorithms before communicating with IoT devices
  - **Data in motion -** value extracted from data while it is being generated



4.3 Chapter Summary

Summary

- Personal information related to health, location, wealth, personal preferences and behaviors is passing through the IoT devices in increasing volumes. This increase in volume elevates the relevance of increasing the attention on data privacy and data protection.
- New wireless technologies and protocols, such as ZigBee, Bluetooth, 4G/4G, and LoRaWAN, have been developed to accommodate the diversity of IoT devices. Wireless technology is selected based on the range of coverage, bandwidth requirements, power consumption, and deployment location.
- Wireless security considerations include: selecting a secure protocol, protection for management frames, identification of frequency jamming, detecting rogue access points, and using security at the application layer.
- Cloud computing is a service that offers off-premise, on-demand access to a shared pool of configurable computing resources. Cloud computing offers services such as IaaS, PaaS, mPaaS and SaaS.
- A fog computing model identifies a distributed computing infrastructure closer to the network edge. It enables edge devices to run applications locally and make immediate decisions.
- The proliferation of devices in the IoT is one of the primary reasons for the exponential growth in data generation. Data can be deemed at rest or in motion. Big Data is typically characterized in three dimensions: volume, velocity, and variety.
- Data stored in servers must be encrypted to avoid data tampering or theft. Regular backups are mandatory to minimize losses in case of a disaster
- IoT devices should run the latest version of firmware and protocols and any communication between devices should be done using protocols that provide secure encryption by default.


CISCO
EDUCATION SERVICE CENTER
REGION 11
Academy Support/Instructor Training Center


CISCO


EDUCATION SERVICE CENTER
REGION 11
Academy Support/Instructor Training Center