Internet of Things - Unit 3

Unit -3

Topics to be covered

Design Principles for Web Connectivity: Web Communication Protocols for connected devices, Message Communication Protocols for connected devices, SOAP, REST, HTTP Restful and Web Sockets. Internet Connectivity Principles: Internet Connectivity, Internet based communication, IP addressing in IOT, Media Access control.

Web Communication Protocols for connected devices-The protocols are used for communication between machines or between a machine and server. Due to constraints in processing capabilities and the low power requirements of IoT devices (which are generally meant to be deployed in environments with constant battery power) with limited bandwidth capabilities, a need was felt for dedicated standards and protocols especially designed for IoT. Since those who manufacture IoT devices and those who create the IoT platforms are different, this required industry standards and protocols that were not high on power consumption, bandwidth usage, or processing power and could be adopted easily by all IoT players— hardware manufacturers, software developers or cloud solutions/service providers.

List of IoT communication protocols:

.

CoAP (Constrained Application Protocol)-Constrained Application Protocol (CoAP) is an Internet application protocol for constrained devices (defined in RFC 7228). It enables constrained devices to communicate with the wider Internet using similar protocols. CoAP is designed for use between devices on the same constrained network, between devices and general nodes on the Internet, and between devices on different constrained networks joined by the Internet. It is an application layer protocol designed for network constrained IoT devices like wireless sensor network nodes, and is often termed the lightweight version of HTTP with support for REST APIs. It can run on most devices that support UDP or a UDP analogue.

· **Bluetooth and Bluetooth Low Energy-**While MQTT and CoAP are infrastructure-independent, which means that it doesn't matter whether you're connected to a wired or a wireless network, Bluetooth provides only wireless communication over radio frequency (2.4GHz spectrum in the ISM band) using an industry standard that was initially used to share files between mobile phones and is now powerful enough to play music (Advanced Audio Distribution Profile/A2DP), stream data, or build your next IoT device. Bluetooth, generally, is divided into three categories.

o **Bluetooth Classic:** This is meant for high data rate applications like streaming audio wirelessly.

o **Bluetooth Smart or Low Energy/BLE:** This is meant for low powered battery-operated devices that stream low packets of data.

o **Bluetooth SmartReady:** These are essentially the 'hub' devices such as computers, smartphones, etc. They support both the 'classic' and 'smart' devices.

Bluetooth is a sophisticated *ad hoc* networking protocol, and is now especially designed from the ground up for IoT. It provides a stable connection and communication channel, which is extremely low profile and low powered. An obvious example is fitness trackers, which even though powered on throughout the day, can last for months on a single charge or run on a coin cell battery, all thanks to BLE (Bluetooth Low Energy). Bluetooth Classic has fixed profiles like UART over Bluetooth class and A2DP class for audio streaming. On the other hand, Bluetooth Low Energy provides GATT or Generic Attribute Profile, which allows users to define their own

standardized by the IETF as RFC 6455 in 2011, and the WebSocket API in Web IDL is being standardized by the W3C.

WebSocket is a different TCP protocol from HTTP. Both protocols are located at layer 7 in the OSI model and, as such, depend on TCP at layer 4. Although they are different, RFC 6455 states that WebSocket "is designed to work over HTTP ports 80 and 443 as well as to support HTTP proxies and intermediaries" thus making it compatible with the HTTP protocol. To achieve compatibility, the WebSocket handshake uses the HTTP Upgrade header to change from the HTTP protocol to the WebSocket protocol.

Internet Connectivity-It defines various concepts mentioned below:

Internet Service Providers (ISP)-Internet Service Provider (ISP) is a company offering access to internet. They offer various services:

· Internet Access

· Domain name registration

· Dial-up access

· Leased line access

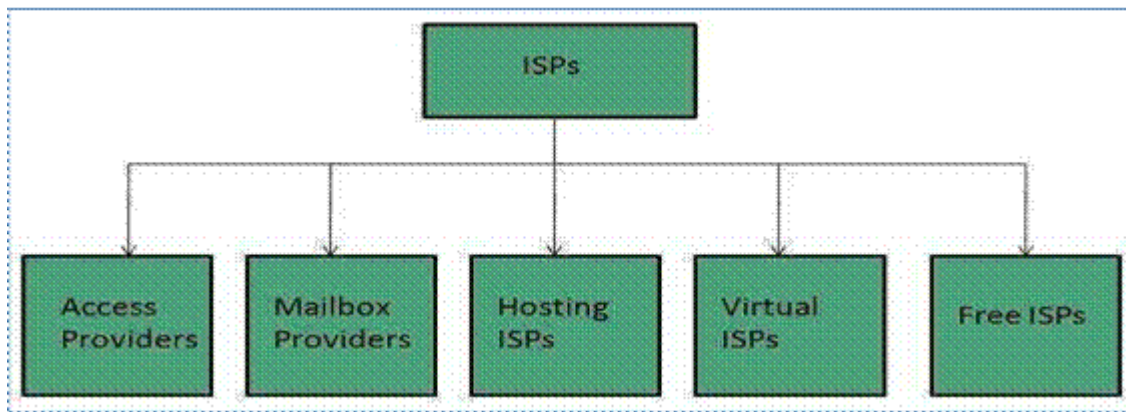**ISP Types-** ISPs can broadly be classified into six categories as shown in the following diagram:

Fig 3.1 ISP Categories

Access Providers-They provide access to internet through telephone lines, cable Wi-Fi or fiber optics.

Mailbox Provider-Such providers offer mailbox hosting services.

Hosting ISPS-Hosting ISPs offers e-mail, and other web hosting services such as virtual machines, clouds etc.

Virtual ISPS-Such ISPs offer internet access via other ISP services.

Free ISPS-Free ISPs do not charge for internet services.

Connection Types-There exists several ways to connect to the internet. Following are these connection types available:

· Dial-up Connection

· ISDN

· DSL

· Cable TV Internet connections

· Satellite Internet connections

· Wireless Internet Connections

profile using Bluetooth, like in the case of a heart rate monitor. BLE is extremely flexible and useful in the IoT space..

Message Communication Protocols for connected devices:

· **MQTT (Message Queue Telemetry Transport)-**It was created about 15 years back for monitoring remote sensor nodes, and is designed to conserve both power and memory. It is based on the 'Publish Subscribe' communication model, where a broker is responsible for relaying messages to MQTT clients. This allows multiple clients to post messages and receive updates on different topics from a central server known as the MQTT broker. This is similar to subscribing to a YouTube channel, where you get notified whenever a new video is posted. Using MQTT, a connected device can subscribe to any number of topics hosted by an MQTT broker.

SOAP-OAP (originally Simple Object Access Protocol) is a protocol specification for exchanging structured information in the implementation of web services in computer networks. Its purpose is to induce extensibility, neutrality and independence. It uses XML Information Set for its message format, and relies on application layer protocols, most often Hypertext Transfer Protocol (HTTP) or Simple Mail Transfer Protocol (SMTP), for message negotiation and transmission.

SOAP allows processes running on disparate operating systems (such as Windows and Linux) to communicate using Extensible Markup Language (XML). Since Web protocols like HTTP are installed and running on all operating systems, SOAP allows clients to invoke web services and receive responses independent of language and platforms. SOAP provides the Messaging Protocol layer of a web services protocol stack for web services. It is an XML-based protocol consisting of three parts:

· an envelope, which defines the message

·

· structure and how to process it

· a set of encoding rules for expressing instances of application-defined datatypes

· a convention for representing procedure calls and responses

SOAP has three major characteristics:

· extensibility (security and Web Services Addressing are among the extensions under development)

· neutrality (SOAP can operate over any protocol such as HTTP, SMTP, TCP, UDP, or Java Message Service)

· independence (SOAP allows for any programming model)

As an example of what SOAP procedures can do, an application can send a SOAP request to a server that has web services enabled—such as a real-estate price database—with the parameters for a search. The server then returns a SOAP response (an XML-formatted

document with the resulting data), e.g., prices, location, features. Since the generated data comes in a standardized machine-parsable format, the requesting application can then integrate it directly.

The SOAP architecture consists of several layers of specifications for:

· Message format

· Message Exchange Patterns (MEP)

· Underlying transport protocol bindings

· Message processing models

· Protocol extensibility

REST-REST (Representational State Transfer) is an architectural style for developing web services. REST is popular due to its simplicity and the fact that it builds upon existing systems and features of the internet's HTTP in order to achieve its objectives, as opposed to creating new standards, frameworks and technologies.

Advantages of REST-A primary benefit of using REST, both from a client and server's perspective, is REST-based interactions happen using constructs that are familiar to anyone who is accustomed to using the internet's Hypertext Transfer Protocol (HTTP).

An example of this arrangement is REST-based interactions all communicate their status using standard HTTP status codes. So, a 404 means a requested resource wasn't found; a 401 code means the request wasn't authorized, a 200 code means everything is OK; and a 500 means there was an unrecoverable application error on the server. Similarly, details such as encryption and data transport integrity are solved not by adding new frameworks or technologies, but instead by relying on well-known Secure Sockets Layer (SSL) encryption and Transport Layer Security (TLS).

Disadvantages of REST-The benefit of REST using HTTP constructs also creates restrictions, however. Many of the limitations of HTTP likewise turn into shortcomings of the REST architectural style. For example, HTTP does not store state-based information between request-response cycles, which means REST-based applications must be stateless and any state management tasks must be performed by the client.

HTTP Restful-In REST architecture, a REST Server simply provides access to resources and the REST client accesses and presents the resources. Here each resource is identified by URIs/ Global IDs. REST uses various representations to represent a resource like Text, JSON and XML. JSON is now the most popular format being used in Web Services.

HTTP Methods

The following HTTP methods are most commonly used in REST based architecture.

· GET – Provides a read only access to a resource.

- PUT – Used to create a new resource.

- DELETE – Used to remove a resource.

- POST – Used to update an existing resource or create a new resource.

- OPTIONS – Used to get the supported operations on a resource.

Restful Web Services-A web service is a collection of open protocols and standards used for exchanging data between applications or systems. Software applications written in various programming languages and running on various platforms can use web services to exchange data over computer networks like the Internet in a manner similar to inter-process communication on a single computer. This interoperability (e.g., between Java and Python, or Windows and Linux applications) is due to the use of open standards. Web services based on REST Architecture are known as Restful Web Services.

Web Sockets- WebSocket is a computer communications protocol, providing full- duplex communication channels over a single TCP connection. The WebSocket protocol was

Dial-up Connection-Dial-up connection uses telephone line to connect PC to the internet. It requires a modem to setup dial-up connection. This modem works as an interface between PC and the telephone line. There is also a communication program that instructs the modem to make a call to specific number provided by an ISP.

Dial-up connection uses either of the following protocols:

- Serial Line Internet Protocol (SLIP)

- Point to Point Protocol (PPP)

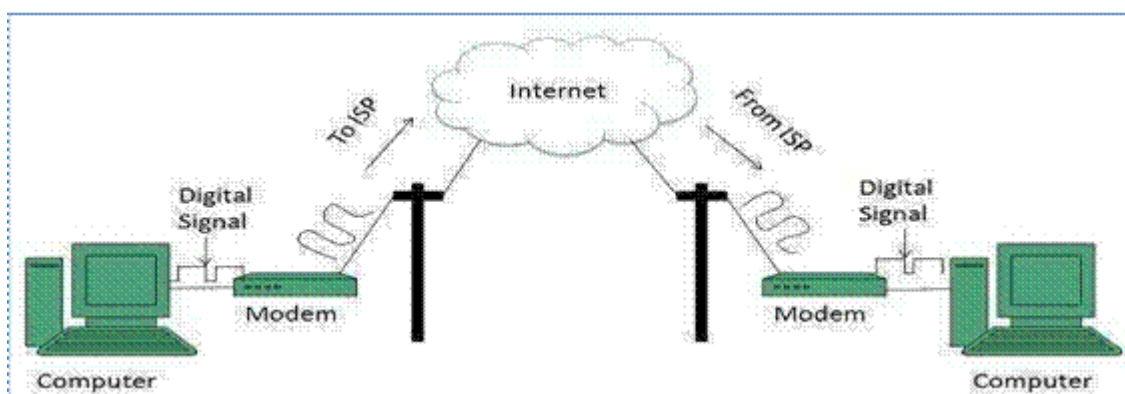The following diagram shows the accessing internet using modem:

Fig 3.2.1 Dial-up connections

ISDN-ISDN is acronym of Integrated Services Digital Network. It establishes the connection using the phone lines which carry digital signals instead of analog signals.

There are two techniques to deliver ISDN services:

· Basic Rate Interface (BRI)

· Primary Rate Interface (PRI)

Key points:

· The BRI ISDN consists of three distinct channels on a single ISDN line: t10 64kbps B (Bearer) channel and one 16kbps D (Delta or Data) channels.

· The PRI ISDN consists of 23 B channels and one D channels with both have operating capacity of 64kbps individually making a total transmission rate of 1.54Mbps.

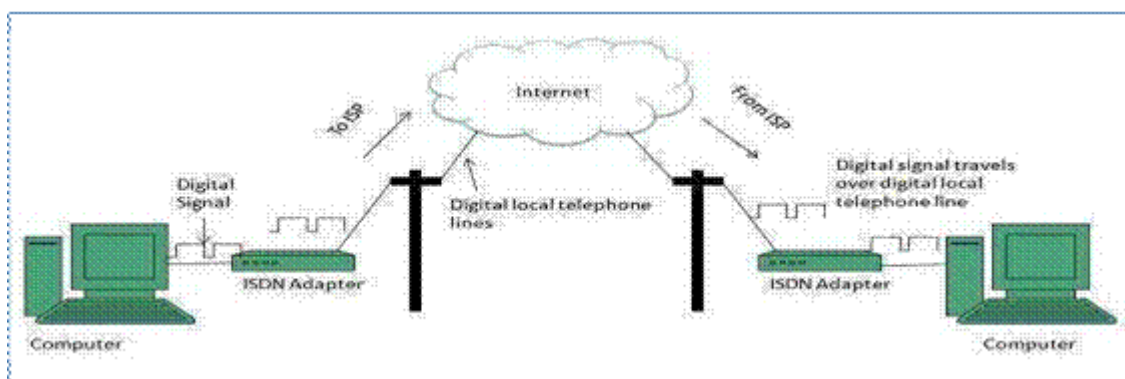The following diagram shows accessing internet using ISDN connection:

Fig 3.2.2 ISDN Connections

DSL-DSL is acronym of Digital Subscriber Line. It is a form of broadband connection as it provides connection over ordinary telephone lines.

Following are the several versions of DSL technique available today:

· Asymmetric DSL (ADSL)

· Symmetric DSL (SDSL)

· High bit-rate DSL (HDSL)

· Rate adaptive DSL (RDSL)

· Very high bit-rate DSL (VDSL)

· ISDN DSL (IDSL)

All of the above mentioned technologies differ in their upload and download speed, bit transfer rate and level of service.

The following diagram shows that how we can connect to internet using DSL technology:
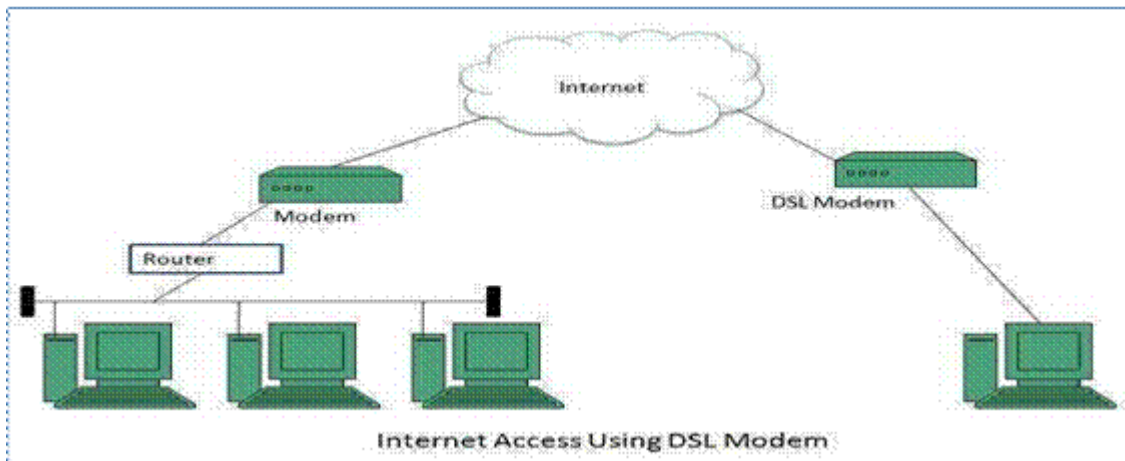

Fig 3.2.3 DSL Connections

Cable TV Internet Connection

Cable TV Internet connection is provided through Cable TV lines. It uses coaxial cable which is capable of transferring data at much higher speed than common telephone line.

Key Points:

· A cable modem is used to access this service, provided by the cable operator.

· The Cable modem comprises of two connections: one for internet service and other for Cable TV signals.

· Since Cable TV internet connections share a set amount of bandwidth with a group of customers, therefore, data transfer rate also depends on number of customers using the internet at the same time.

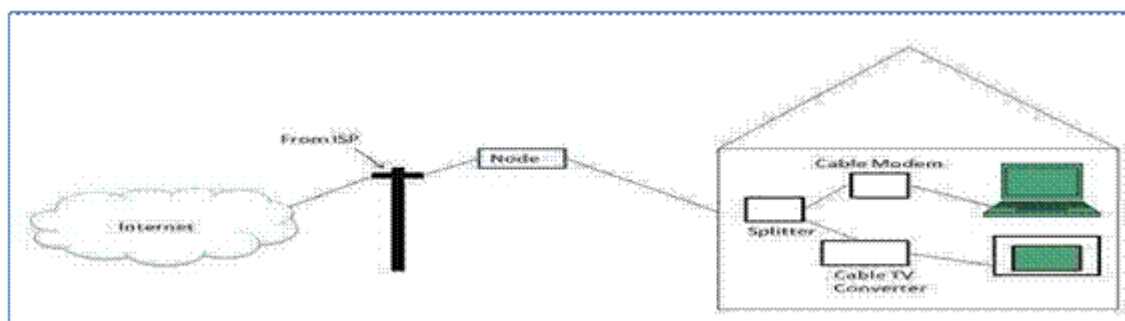The following diagram shows that how internet is accessed using Cable TV connection:

Fig 3.2.4 Cable TV Connections

Satellite Internet Connection-Satellite Internet connection offers high speed connection to the internet. There are two types of satellite internet connection: one way connection or two way connection.

In one way connection, we can only download data but if we want to upload, we need a dialup access through ISP over telephone line.

In two way connection, we can download and upload the data by the satellite. It does not require any dialup connection.

The following diagram shows how internet is accessed using satellite internet connection:
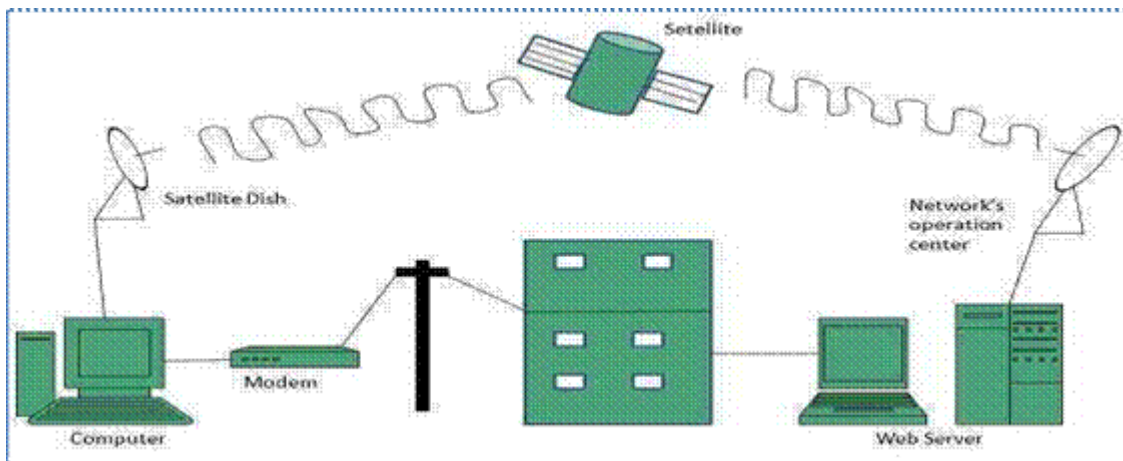

Fig 3.2.5 Satellite Connections

Wireless Internet Connection-Wireless Internet Connection makes use of radio frequency bands to connect to the internet and offers a very high speed. The wireless internet connection can be obtained by either Wi-Fi or Bluetooth.
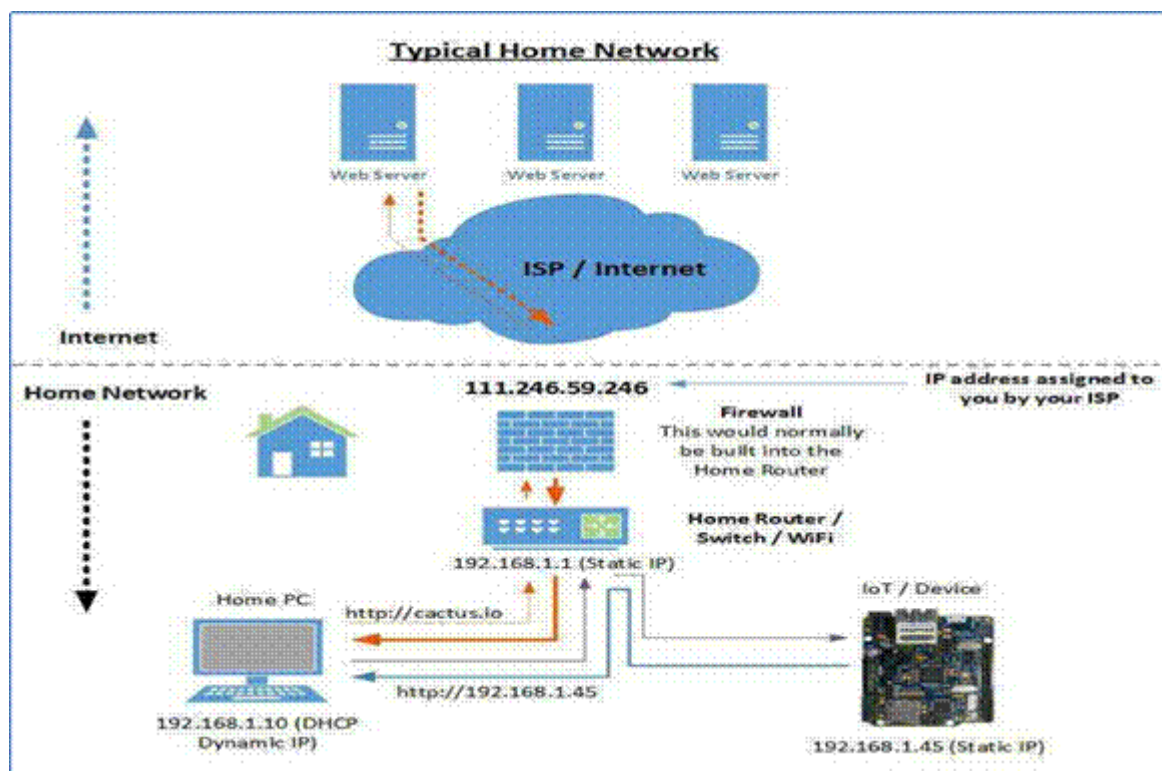
Key Points:

· Wi-Fi wireless technology is based on IEEE 802.11 standards which allow the electronic device to connect to the internet.

· Bluetooth wireless technology makes use of short-wavelength radio waves and helps to create personal area network (PAN).

Internet based communication-In much of the world the Internet is becoming the primary medium for communication in business. Internet communication tools save money in a variety of ways. Email, instant messaging and social networking are all free. There are many different kinds of Internet communications tool, such as email, VoIP, forums, online chat and social networking among others. Using the latest tools and methods of communicating over the Internet is essential for bringing your business into the modern age of communication and marketing.

VoIP and Internet Telephony-It is common for voice communications to be carried out over the Internet using voice over Internet protocol software. VoIP allows you to call a telephone -- either a fixed or mobile phone -- over the Internet. This is often considerably cheaper than calling from a telephone, particularly with international calls. One of the most popular Internet telephony tools is Skype. With Skype and similar Internet telephony tools, you can conduct free voice conversations between two computers.

· **Email-**The original Internet communication tool, email is still an essential tool every business should have. In spite of this, with the rise of messaging through social networking sites and instant messages, email is not quite as important as it used to be.

· **Social Networking-**Social networking is all about forming groups, sharing online content and exchanging information. In addition to being a major part of social life in the modern world, social networking is an invaluable tool for Internet marketing since it provides a user-friendly and highly accessible platform upon which to exchange information on products and services. For example, if someone likes an article on your business blog or website, he may decide to share it with his friends over Facebook or Twitter.

· **Forums-**Forums, like email, have also been around since the dawn of the Internet. Forums provide a place to exchange messages and participate in conversations. The main differences from instant messaging are that forums are generally public and the communications are not in real time. Forums and their regular posters and readers form communities that can be valuable to your business.

IP addressing in IOT- We can connect Internet of Thing or device to the Internet. How we connect depends ultimately on what we actually want to do with the device. Shown below is a typical home network. This would normally consist of a router / firewall that connect to your ISP (Internet Service Provider). The connection to your ISP could by via ADSL or Ethernet using a fiber service for example.

Fig 3.3 IP addressing in Home Networks

When the home router connects to the ISP it will be assigned an IP address which is what is used to communicate with servers or other service on the Internet. This is a public IP address and is addressable by the internet. In the diagram above the public IP address is 111.246.59.246.

This is your public IP address you used to connect to the cactus.io server to view this page.**182.73.155.114**

(If there is more than one IP then you might be connecting using a proxy server or VPN service), be aware that this IP address will change every time that your home router is rebooted or reconnects to the ISP. Some ISP's allow you to pay extra for a fixed IP address. However most will not for home internet services.

Connect to a Web Server-When we enter a URL into our browser it will use a DNS server to convert the name to an IP address. The DNS server would normally be provided by your ISP. In the example above we are using cactus.io for the URL. The DNS server would then return the IP address of 104.130.130.228. The browser will then try to connect to the server via the router. The router will connect to the remote server using the public IP address assigned to your router. The server hosting cactus.io will then send data back to your router using your public ip address (111.246.59.246). The router will then transmit this data back to your PC using the private IP address of 192.168.1.10.
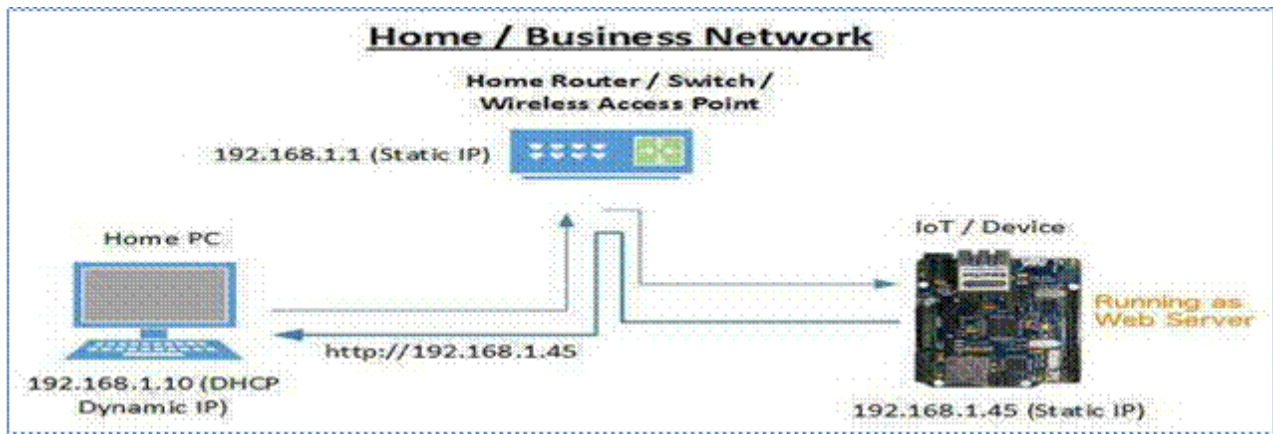
Connect to an Internal IoT Device-We can connect to a web server running on our IoT device by entering the IP address of http://192.168.1.45 into the browser URL. The connection will be made in this case via the switch built into the home router. The switch knows what port the IoT device is connected to and transmits and receives data via this port. The router has no role in this network request as it's a private IP address and the PC and IoT device are on the same network.

How to connect my device to the Internet

This all depends on the role of the device and we have the following options:

· Option 1) We access this device only on the home / business network

· Option 2) The device only connects to a local / remote server

· Option 3) We access this device from the Internet using a Static Public IP Address

· Option 4) We access this device from the Internet using a Dynamic Public IP Address

Home / Business Network

Home Router / Switch / Wireless Access Point

192.168.1.1 (Static IP)

Home PC

http://192.168.1.45

192.168.1.10 (DHCP Dynamic IP)

IoT / Device

Running as Web Server

192.168.1.45 (Static IP)

Option 1) Access this device only on the home / business network-In this scenario the IoT device is configuring as a server. The easiest way is to assign a static IP address. This address is coded into the sketch.

Fig 3.4 IP addressing in Business Network

—
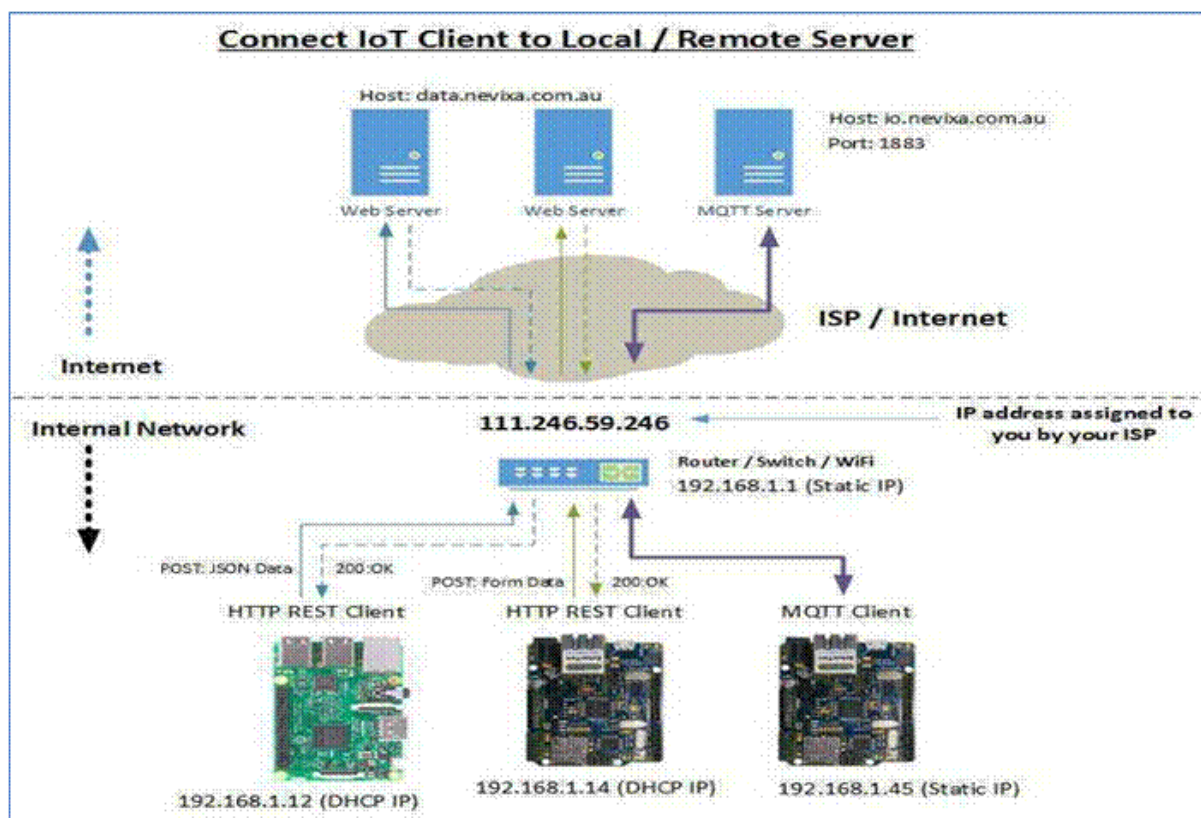
When a client connects to the IoT device it passes through the switch and out to the device it is connected to. No routing is required here.

Option 2) Device connects to a local / remote server-For this scenario the IoT device initiates a connection to a local or remote server. This could be using a http REST POST or configured as MQTT client. It could also be a custom connection method as long as it initiates the connection to the remote service.

Because the device is creating the connection it allows us to use DHCP and a dynamically assigned IP address.

Fig 3.5 Client-Server Communication

In the diagram above two of the devices send a HTTP REST Post to a server in the cloud. If the remote server accepts the connection and data it will generally respond with a 200 OK. The client will then close the connection until the next post is sent.

Option 3) Access the Device from the Internet with Static Public IP Address

The world is running out of IPV4 IP addresses. This means ISP's are pretty strict on giving out static IP addresses. It's much easier for them to use a dynamic pool of IP addresses to assign to their clients.

Generally home internet services are not available with a static IP address. However you might be able to pay extra for this functionality. Some business accounts are available with a static IP address. The most common reason for wanting a static ip is for hosting a email server.

—
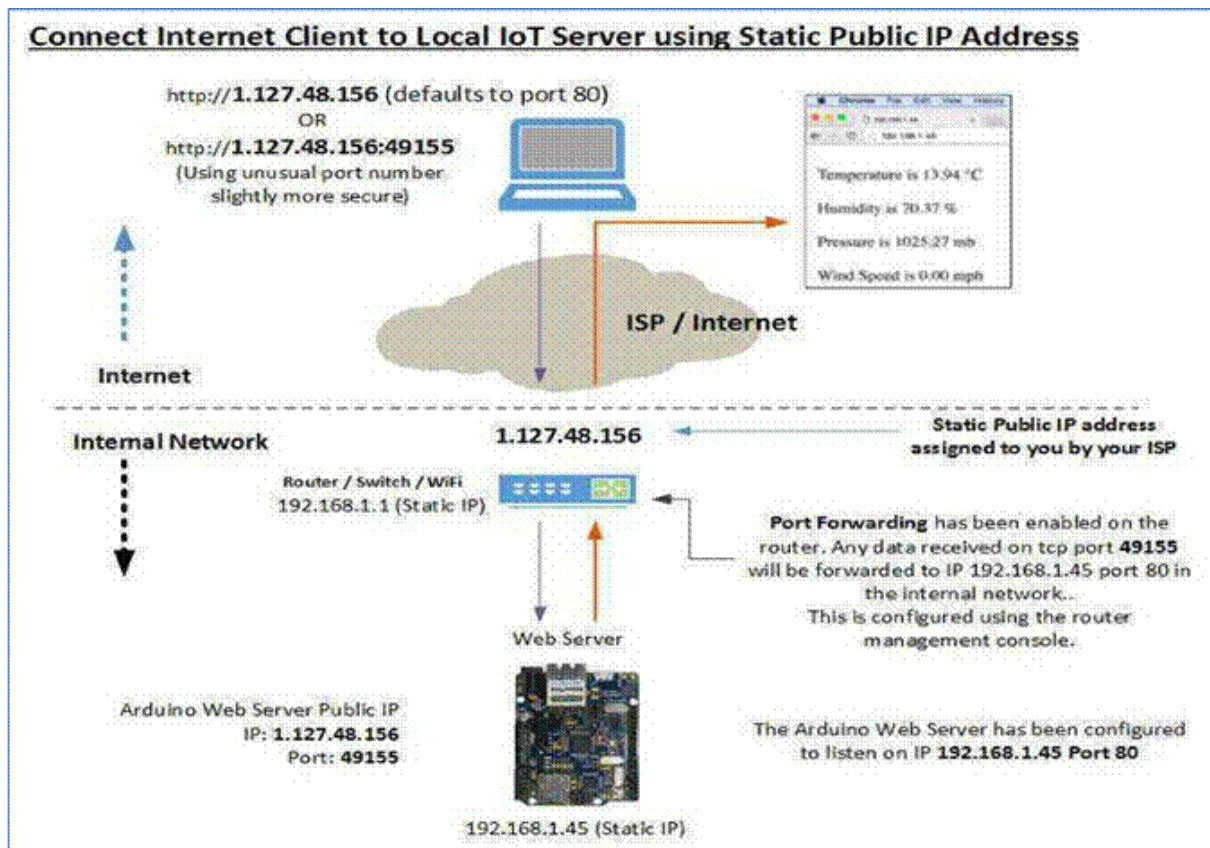
In this diagram above we could use http://1.127.48.156 or http://1.127.48.156:49155 to connect to the IoT server. In the first URL we do not specify a port number so the browser will use the default port of 80. In the second URL we use the port 49155. By using a random private port number we improve the security for our IoT server. If someone does a port scan they will always check port 80 as it's a default. They might not bother scanning private port numbers

If you have multiple IoT devices you can setup port forwarding on the router to recognize different port numbers.

Option 4) Access the Device from the Internet with Dynamic Public IP Address-One of the most common ways of dealing with a dynamic public (WAN) IP addresses is to use a Dynamic DNS Service provider. Some of these services are free but most require a monthly payment. Most routers these days support third party Dynamic DNS service providers. You configure the router with the provider, username and password. When the router detects a WAN interface IP address change it updates the DDNS service provider with the new IP details.
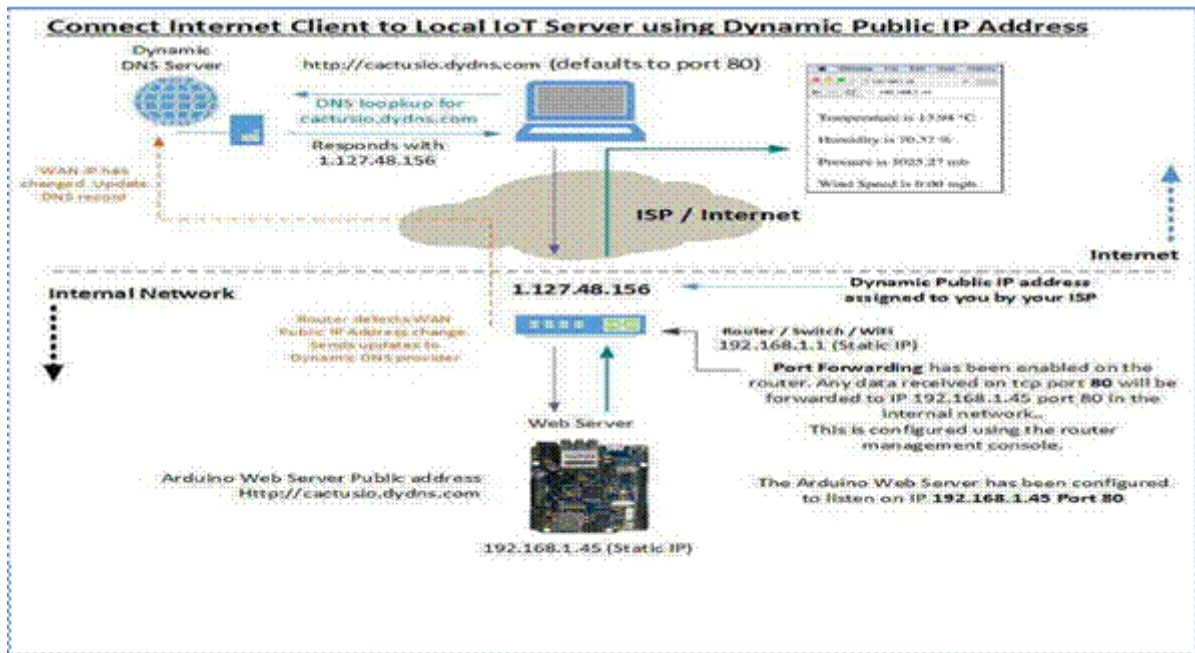

Fig 3.7 Public IP Addressing

When you sign up with one of these providers you provide a domain name you would like to use. In the example below the name we used is cactusio. This is a sub domain for dydns.com. When we enter http://cactusio.dydns.com into the browser it will do a dnslookup on cactusio.dydns.com. If it's a valid domain it will respond with the IP address which just happens to be the public (WAN) IP address of the home / office router.

The office router will detect the data packet matches a record in the port forwarding table and pass the data onto the IoT device using the static IP of 192.168.1.45. The IoT device will respond with the appropriate html to view in the internet client browser.

Media Access control

In Layer 2 of a network, the Media Access Control (MAC) sub-layer provides addressing and channel access control mechanisms that enable several terminals or network nodes to communicate in a network.

The MAC sub-layer acts as an interface between the logical link control (LLC) Ethernet sub-layer and Layer 1 (the physical layer). The MAC sub-layer emulates a full-duplex logi

communication channel in a multipoint network. This channel may provide unicast, multicast or broadcast communication service. The MAC sub-layer uses MAC protocols to prevent collisions. In Layer 2, multiple devices on the same physical link can uniquely identify one another at the data link layer, by using the MAC addresses that are assigned to all ports on a switch. A MAC algorithm accepts as input a secret key and an arbitrary-length message to be authenticated, and outputs a MAC address.