IoT Data Link Communication Protocol

The IoT Data Link communication protocol provides service to the Network Layer. There are various protocols and standard technologies specified by the different organization for data link protocols.

WirelessHART

What is HART technology?

HART (Highway Addressable Remote Transducer) Protocol is **an open standard used globally to send and receive digital information using analog wiring between smart devices and control systems**. ... The HART Protocol defines physical connection technology as well as commands used by applications.

WirelessHART uses a **2.4 GHz band**—license-free and used worldwide—as a transfer medium for several radio technologies, including WLAN, Bluetooth, and ZigBee. But, **WirelessHART** is much more than a WLAN variant.
WirelessHART uses a **flat mesh network** where all radio stations (field devices) form a network. Every participating station serves simultaneously as a **signal source** and a **repeater**. The original transmitter sends a message to its nearest neighbor, which passes the message on until the message reaches the base station and the actual receiver. In addition, **alternative routes** are set up in the initialization phase. If the message cannot be transmitted on a particular path, due to an obstacle or a defective receiver, the message is automatically passed to an alternative route. So, in addition to extending the range of the network, the **flat mesh network** provides redundant communication routes to increase reliability.
The communication in the **Wireless Network** is coordinated with TDMA (Time Division Multiple Access), which synchronizes the network participants in 10 ms timeframes. This enables a very reliable (collision-free) network, and reduces the lead and lag times during which a station must be active.
To avoid jamming, **WirelessHART** uses also FHSS (Frequency Hopping Spread Spectrum). All 15 channels as defined in IEEE802.15.4 are used in parallel; **WirelessHART** uses FHSS to “hop” across these channels. Channels that are already in use are blacked out to avoid collisions with other wireless communication systems.

The combination of 10s synchronization and 15 channels allows 1500 communications per second.

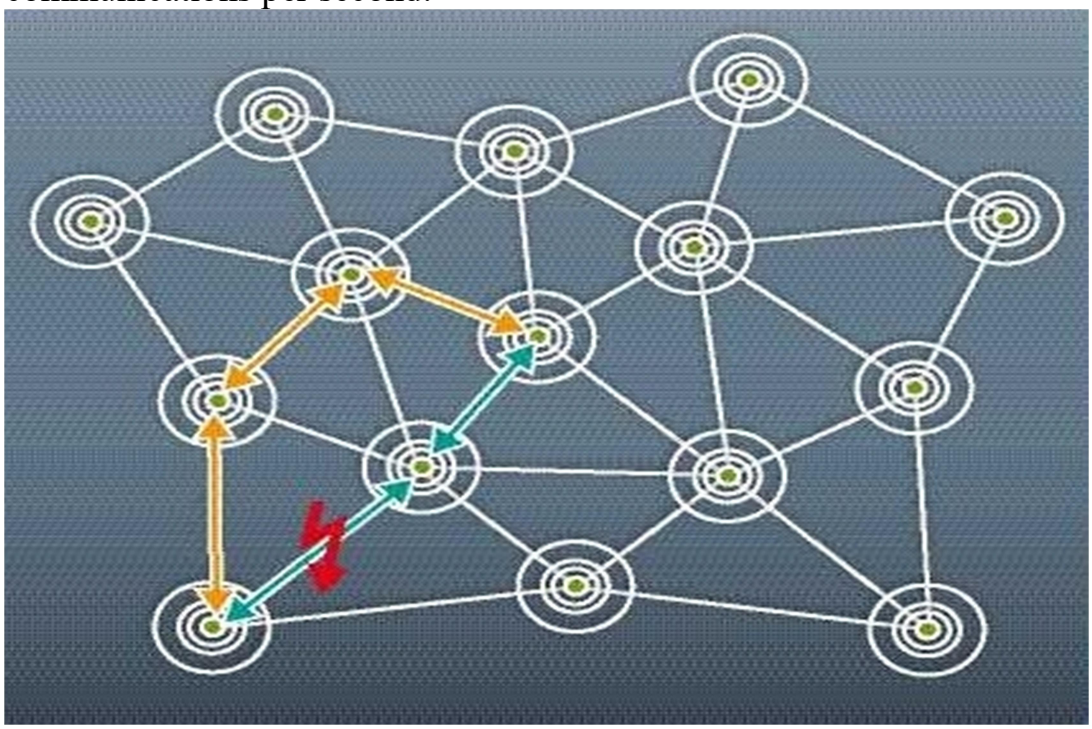


Figure- WirelessHART mesh network topology

Bluetooth

Bluetooth is a short-range wireless communication network over a radio frequency. Bluetooth is mostly integrated into smartphones and mobile devices. The Bluetooth communication network works within 2.4 ISM band frequencies with data rate up to 3Mbps.

There are three categories of Bluetooth technology:

1. Bluetooth Classic
2. Bluetooth Low Energy
3. Bluetooth SmartReady

The features of Bluetooth 5.0 version is introduced as Bluetooth 5 which have been developed entirely for the Internet of Things.

Properties of Bluetooth network

- **Standard:** Bluetooth 4.2
- **Frequency:** 2.4GHz
- **Range:** 50-150m

- **Data transfer rates:** 3Mbps

Advantages of Bluetooth network

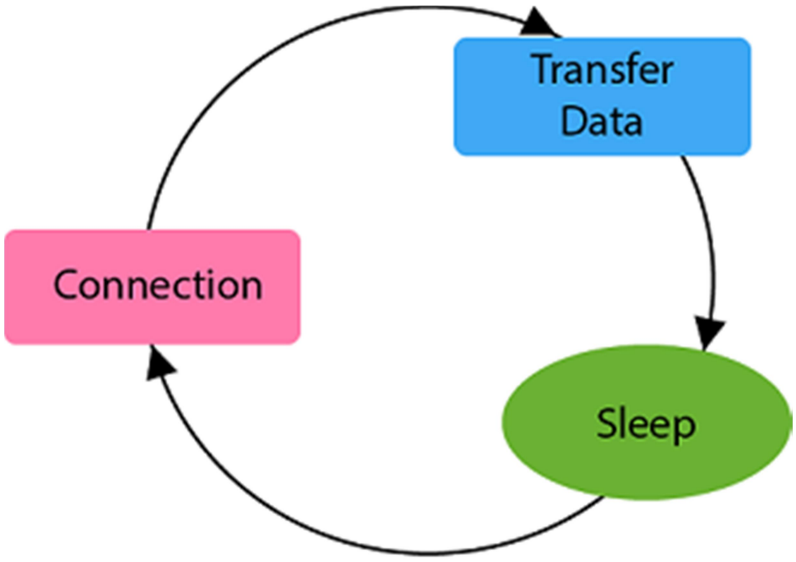
- It is wireless.
- It is cheap.
- It is easy to install.
- It is free to use if the device is installed with it.

Disadvantages of Bluetooth network

- It is a short-range communication network.
- It connects only two devices at a time.

Bluetooth Low Energy

Bluetooth low energy (BLE) is a short-range communication network protocol with PHY (physical layer) and MAC (Medium Access Control) layer. It is designed for low-power devices which uses less data. BLE always remain in sleep mode except when the connection between devices is initiated and data transmission occurs, due to this it conserves power of the device. Bluetooth low energy follows the master/slave architecture and offers two types of frames that are adverting and data frames. Slave node sent the advertising frame to discover one or more dedicated advertisement channels. Master nodes sense this advertisement channels to find slaves and connect them.



BLE Technology

Z-Wave

Z-Wave is a wireless communication protocol with the frequency of 900MHz. The ranges of Z-Wave lies between 30 meters to 100 meters with the data transfer rate of 100kbps so that it is suitable for small messages in IoT applications for home automation. This communication protocol operates on mesh network architecture with one and several secondary controllers.

Properties of Z-Wave protocol

- **Standard:** Z-Wave Alliance ZAD12837 / ITU-T G.9959
- **Frequency:** 908.42GHz
- **Range:** 30-100m
- **Data transfer rate:** 100kbps

Advantages of Z-Wave protocol

- Low power consumption
- Remote or local control
- Simple installation
- Interoperability

Application of Z-Wave protocol

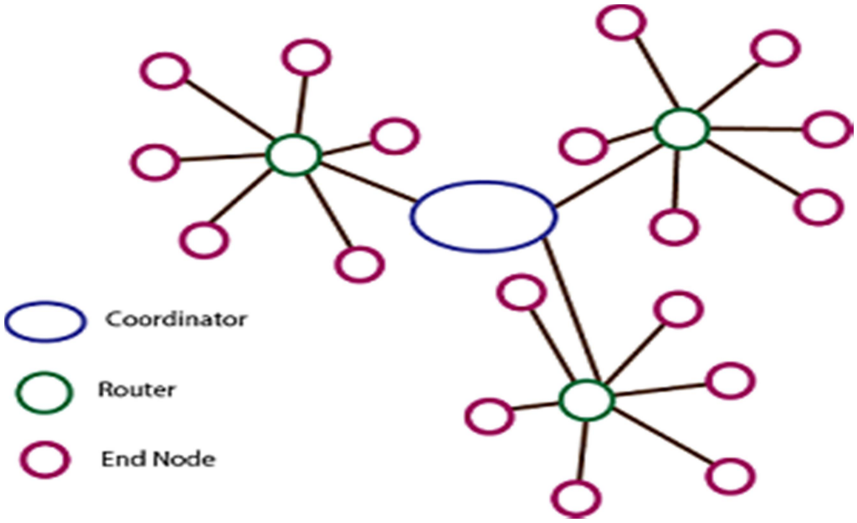
- Smart product and IoT based application
- Energy saving
- Home security

ZigBee Smart Energy

ZigBee is a low power, low data rate wireless personal area network communication protocol. It is mostly used in home automation and industrial settings. Since ZigBee is a low power communication protocol, the IoT power devices used with ZigBee technology. The ZigBee communication protocol is based on the IEEE 802.15.4 standard operating at the 2.4GHz frequency. The ZigBee protocol supports star, cluster or wireless mesh technology topology.

ZigBee uses the following devices in its network:

- Zigbee Coordinator
- Zigbee End Device
- Zigbee Router



Properties of ZigBee protocol

- **Standard:** ZigBee 3.0 based on IEEE802.15.4
- **Frequency:** 2.4GHz
- **Range:** 10-100m
- **Data transfer rate:** 250kbps

Advantages of ZigBee protocol

- Wireless
- Mesh networking
- Direct communication

- Low power consumption

Disadvantages of ZigBee protocol

- Costly
- Works with low speed within a small distance

Application of ZigBee protocol

- Commercial and residential control
- Personal and healthcare
- Home networking
- Industrial control and management
- Consumer electronics

LoRaWAN

LoRaWAN refers to Long Rage Wide Area Network which is a wide area network protocol. It is an optimized low-power consumption protocol design to support large-scale public networks with millions of low-power devices. A single operator operates the LoRaWAN. The LoRaWAN network is a bi-directional communication for IoT application with low cost, mobility, and security.

Properties of LoRaWAN protocol

- **Standard:** LoRaWAN
- **Frequency:** Various
- **Range:** 2-5km (urban environment), 15km (suburban environment)
- **Data Rates:** 0.3-50 kbps.

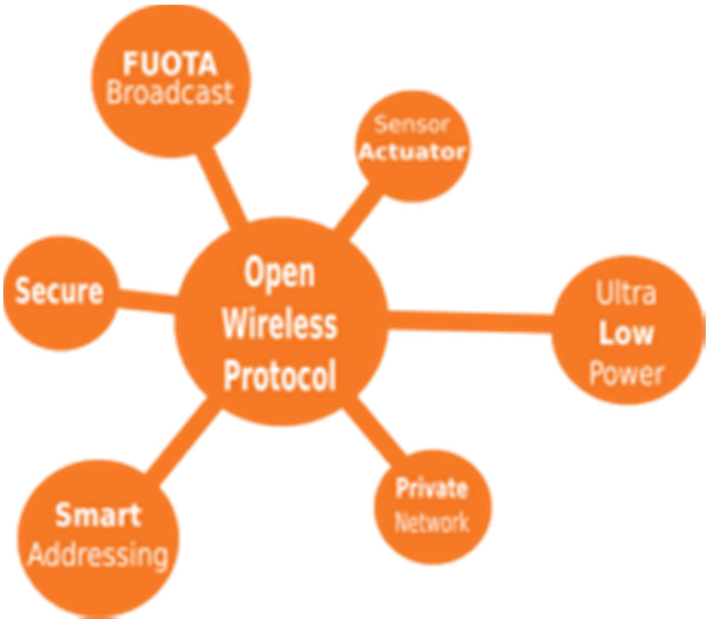
DASH7

DASH7 is an “instant-on,” long-range, low power wireless communications standard for applications requiring modest bandwidth like text messages, sensor readings, or location-based advertising coordinates.

The DASH7 Alliance Protocol (D7A) is an Open Standard for bi-directional, sub-Ghz medium range wireless communication tailored for ultra lower sensor-actuator applications using private networks. D7A stems from ISO 18000-7 for Active RFID and operates in the sub-GHz ISM bands. The protocol specification is free to use without any patent or licence requirements. You can freely download the latest D7A version 1.2 specifications from this website.

Sensors will securely report events and actuators can receive commands with a typical latency of 1 second while consuming only 30 uA on average. It's local synchronisation and smart addressing features allow to upgrade thousands of sensors simultaneously, drastically reducing the upgrade time.

D7A fills the gap between the Short and the Large Area Networks. D7A excels in urban and industrial network installations connecting actuators and messaging applications (sensors, alarms, states) with ranges up to 500 m.



BLAST networking technology

Networks based on DASH7 differ from typical wire-line and wireless networks utilizing a "session". DASH7 networks serves applications in which low power usage is essential and data transmission is typically much slower and/or sporadic, like basic telemetry. Thus instead of replicating a wire-line "session", DASH7 was designed with the concept of **B.L.A.S.T.**:

- **B**ursty: Data transfer is abrupt and does not include content such as video, audio, or other isochronous forms of data.

- **L**ight: For most applications, packet sizes are limited to 256 bytes. Transmission of multiple consecutive packets may occur but is generally avoided if possible.
- **A**synchronous: DASH7's main method of communication is by command–response, which by design requires no periodic network "hand-shaking" or synchronization between devices.
- **S**tealth: DASH7 devices does not need periodic beaconing to be able to respond in communication.
- **T**ransitive: A DASH7 system of devices is inherently mobile or transitional. Unlike other wireless technologies, DASH7 is upload-centric, not download-centric, thus devices do not need to be managed extensively by fixed infrastructure (i.e. base stations).

Sub 1-GHz

D7A utilizes the 433, 868 and 916 MHz frequencies,[5] which is globally available and license-free.

Sub 1-GHz is ideal for wireless sensor networking applications, since it penetrates concrete and water, but also has the ability to transmit/receive over very long ranges without requiring a large power draw on a battery. The low input current of typical tag configurations allows powering on coin cell or thin-film batteries.

Tag-to-tag communications

Unlike most active RFID or LPWAN technologies, DASH7 supports tag-to-tag communications.

Localization

Localization techniques can be applied to DASH7 endpoints. An accuracy of 1 m using DASH7 beacons at 433 MHz has been achieved in a lab experiment.

Integrated query protocol

DASH7 supports a built-in query protocol that minimizes "round trips" for most messaging applications that results in lower latency and higher network throughput.

Range

DASH7 provides a link budget of up to 140 dB with 27 dBm transmission power, which positions the technology as medium-range, compared to short-range (Bluetooth, Wi-Fi, ...) and long-range (LoRaWAN, SigFox). Note that higher ranges are always obtained at the expense of per-bit power consumption and transmission duration. Low-power long-range technologies are generally not truly bi-directional, as the regular scanning duty is pretty high. In this context, DASH7 is a very good compromise between range, power

consumption, and bi-directionality and is very suitable for industrial applications with effective range of 100 to 500 m.

In line-of-sight situations, DASH7 devices today advertise read ranges of 1 kilometer or more, however, ranges of up to 10 km have been tested by Savi Technology and are easily achievable in the European Union, where governmental regulations are less constrained than in the USA.

Interoperability

The DASH7 Alliance is currently working on a certification program that tests functionally the DASH7 devices. The certification is composed of a set of test scenarios covering transactions in different stack configurations (channel, QoS, security). The physical wireless interface is not covered by the certification and will have to comply to local radio regulations.

Alternative modulations

The DASH7 Alliance policy does not allow to add proprietary or licensable modulation techniques in the official DASH7 Alliance Protocol. However, the layered structure of the protocol allows simple integration of alternative modulations, such as LoRa, under the network layer (D7ANL).

Applications

Commercial applications

Similar to other networking technologies that began with defence sector (e.g. DARPA funding the Internet), DASH7 is similarly suited to a wide range of applications in development or being deployed including:

- **Building automation**, **access control**, **smart energy**. DASH7's signal propagation characteristics allow it to penetrate walls, windows, doors, and other substances that serve as impediments to other technologies operating at 2.45 GHz, for example. For smart energy and building automation applications, DASH7 networks can be deployed with far less infrastructure than competing technologies and at far lower total cost of ownership.
- **Location-based services** DASH7 is being used today for developing new location-based services using a range of DASH7-enabled devices including smartcards, keyfobs, tickets, watches and other conventional products that can take advantage of the unique small footprint, low power, long range, and low cost of DASH7 relative to less practical and high-power wireless technologies like Wi-Fi or Bluetooth. Using DASH7, users can "check in" to venues in ways not practical with current check-in technologies like GPS, that are power-intensive and fail indoors and in urban environments. Location-based services like Foursquare, Novitaz, or Facebook can exploit

this capability in DASH7 and award loyalty points, allow users to view the Facebook or Twitter addresses of those walking past, and more.[7]

- **Mobile advertising** DASH7 is being developed for "smart" billboards and kiosks, likewise "smart" posters that can be ready from many meters (or even kilometers) away, creating new opportunities for both tracking the effectiveness of advertising spend but also creating new e-commerce opportunities. DASH7's potential to automate check-ins and check-outs provides essential infrastructure to location-based advertising and promotions
- **Automotive** DASH7 is increasingly seen as the next-generation tire pressure monitoring system given its operation at the same frequency (433 MHz) as nearly all proprietary TPMS systems today. DASH7-based TPMS will provide end users with more accurate tire pressure readings, resulting in greater fuel economy, reduced tire wear and tear, and greater safety. DASH7 products are also being designed and used for other automotive applications like supply chain visibility.
- **Logistics** DASH7 is being used today for tracking the whereabouts of shipping containers, pallets, roll cages, trucks, rail cars, maritime vessels, and other supply chain assets, providing businesses with unprecedented visibility into their everyday operations. Also cold chain management (vaccines, fresh produce, cut flowers, etc.), whereby DASH7 is used for monitoring the in-transit temperature and other environmental factors that can impact the integrity of sensitive products.

IoT Network Layer Protocols

The network layer is divided into two sublayers: routing layer which handles the transfer of packets from source to destination, and an encapsulation layer that forms the packets.

What is IP?

An IP stands for internet protocol. An IP address is assigned to each device connected to a network. Each device uses an IP address for communication. It also behaves as an identifier as this address is used to identify the device on a network. It defines the technical format of the packets. Mainly, both the networks, i.e., IP and TCP, are combined together, so together, they are referred to as a TCP/IP. It creates a virtual connection between the source and the destination.

We can also define an IP address as a numeric address assigned to each device on a network. An IP address is assigned to each device so that the device on a network can be identified uniquely. To facilitate the routing of packets, TCP/IP protocol uses a 32-bit logical address known as IPv4(Internet Protocol version 4).

An IP address consists of two parts, i.e., the first one is a network address, and the other one is a host address.

- There are two types of IP addresses:
- IPv4
- IPv6

What is IPv4?

IPv4 is a version 4 of IP. It is a current version and the most commonly used IP address. It is a 32-bit address written in four numbers separated by 'dot', i.e., periods. This address is unique for each device.

For example, **66.94.29.13**

The above example represents the IP address in which each group of numbers separated by periods is called an Octet. Each number in an octet is in the range from 0-255. This address can produce 4,294,967,296 possible unique addresses.

In today's computer network world, computers do not understand the IP addresses in the standard numeric format as the computers understand the

numbers in binary form only. The binary number can be either 1 or 0. The IPv4 consists of four sets, and these sets represent the octet. The bits in each octet represent a number.

Each bit in an octet can be either 1 or 0. If the bit the 1, then the number it represents will count, and if the bit is 0, then the number it represents does not count.

Representation of 8 Bit Octet

128	64	32	16	8	4	2	1

The above representation shows the structure of 8- bit octet.

Now, we will see how to obtain the binary representation of the above IP address, i.e., 66.94.29.13

Step 1: First, we find the binary number of 66.

128	64	32	16	8	4	2	1
0	1	0	0	0	0	1	0

To obtain 66, we put 1 under 64 and 2 as the sum of 64 and 2 is equal to 66 (64+2=66), and the remaining bits will be zero, as shown above. Therefore, the binary bit version of 66 is 01000010.

Step 2: Now, we calculate the binary number of 94.

128	64	32	16	8	4	2	1
0	1	0	1	1	1	1	0

To obtain 94, we put 1 under 64, 16, 8, 4, and 2 as the sum of these numbers is equal to 94, and the remaining bits will be zero. Therefore, the binary bit version of 94 is 01011110.

Step 3: The next number is 29.

128	64	32	16	8	4	2	1
0	0	0	1	1	1	0	0

To obtain 29, we put 1 under 16, 8, 4, and 1 as the sum of these numbers is equal to 29, and the remaining bits will be zero. Therefore, the binary bit version of 29 is 00011101.

Step 4: The last number is 13.

128	64	32	16	8	4	2	1
0	0	0	0	1	1	0	1

To obtain 13, we put 1 under 8, 4, and 1 as the sum of these numbers is equal to 13, and the remaining bits will be zero. Therefore, the binary bit version of 13 is 00001101.

Drawback of IPv4

Currently, the population of the world is 7.6 billion. Every user is having more than one device connected with the internet, and private companies also rely on the internet. As we know that IPv4 produces 4 billion addresses, which are not enough for each device connected to the internet on a planet. Although the various techniques were invented, such as variable- length mask, network address translation, port address translation, classes, inter-domain translation, to conserve the bandwidth of IP address and slow down the depletion of an IP address. In these techniques, public IP is converted into a private IP due to which the user having public IP can also use the internet. But still, this was not so efficient, so it gave rise to the development of the next generation of IP addresses, i.e., IPv6.

What is IPv6?

IPv4 produces 4 billion addresses, and the developers think that these addresses are enough, but they were wrong. IPv6 is the next generation of IP addresses. The main difference between IPv4 and IPv6 is the address size of IP addresses. The IPv4 is a 32-bit address, whereas IPv6 is a 128-bit hexadecimal address. IPv6 provides a large address space, and it contains a simple header as compared to IPv4.

It provides transition strategies that convert IPv4 into IPv6, and these strategies are as follows:

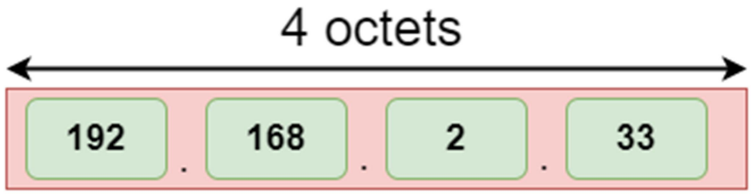
- **Dual stacking:** It allows us to have both the versions, i.e., IPv4 and IPv6, on the same device.
- **Tunneling:** In this approach, all the users have IPv6 communicates with an IPv4 network to reach IPv6.
- **Network Address Translation:** The translation allows the communication between the hosts having a different version of IP.

This hexadecimal address contains both numbers and alphabets. Due to the usage of both the numbers and alphabets, IPv6 is capable of producing over 340 undecillion ($3.4*10^{38}$) addresses.

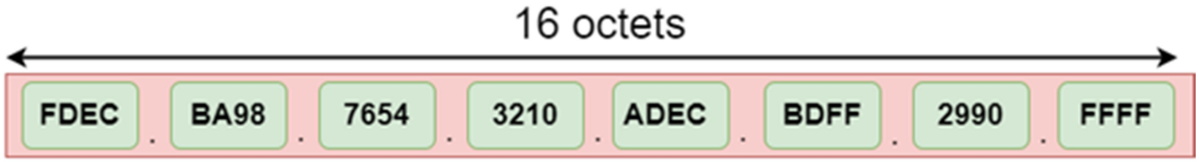
IPv6 is a 128-bit hexadecimal address made up of 8 sets of 16 bits each, and these 8 sets are separated by a colon. In IPv6, each hexadecimal character represents 4 bits. So, we need to convert 4 bits to a hexadecimal number at a time

Address format

The address format of IPv4:



The address format of IPv6:



The above diagram shows the address format of IPv4 and IPv6. An IPv4 is a 32-bit decimal address. It contains 4 octets or fields separated by 'dot', and each field is 8-bit in size. The number that each field contains should be in the range of 0-255. Whereas an IPv6 is a 128-bit hexadecimal address. It contains 8 fields separated by a colon, and each field is 16-bit in size.

Differences between IPv4 and IPv6:-

	Ipv4	Ipv6
Address length	IPv4 is a 32-bit address.	IPv6 is a 128-bit address.
Fields	IPv4 is a numeric address that consists of 4 fields which are separated by dot (.).	IPv6 is an alphanumeric address that consists of 8 fields, which are separated by colon.
Classes	IPv4 has 5 different classes of IP address that includes Class A, Class B, Class C, Class D, and Class E.	IPv6 does not contain classes of IP addresses.
Number of IP address	IPv4 has a limited number of IP addresses.	IPv6 has a large number of IP addresses.
VLSM	It supports VLSM (Virtual Length Subnet Mask). Here, VLSM means that Ipv4 converts IP addresses into a subnet of different sizes.	It does not support VLSM.
Address configuration	It supports manual and DHCP configuration.	It supports manual, DHCP, auto-configuration, and renumbering.
Address space	It generates 4 billion unique addresses	It generates 340 undecillion unique addresses.
End-to-end connection integrity	In IPv4, end-to-end connection integrity is unachievable.	In the case of IPv6, end-to-end connection integrity is achievable.
Security features	In IPv4, security depends on the application. This IP address is not developed in keeping the security feature in mind.	In IPv6, IPSEC is developed for security purposes.
Address representation	In IPv4, the IP address is represented in decimal.	In IPv6, the representation of the IP address in hexadecimal.
Fragmentation	Fragmentation is done by the senders and the forwarding	Fragmentation is done by the senders only.

	routers.	
Packet flow identification	It does not provide any mechanism for packet flow identification.	It uses flow label field in the header for the packet flow identification.
Checksum field	The checksum field is available in IPv4.	The checksum field is not available in IPv6.
Transmission scheme	IPv4 is broadcasting.	On the other hand, IPv6 is multicasting, which provides efficient network operations.
Encryption and Authentication	It does not provide encryption and authentication.	It provides encryption and authentication.
Number of octets	It consists of 4 octets.	It consists of 8 fields, and each field contains 2 octets. Therefore, the total number of octets in IPv6 is 16.

6LoWPAN

The 6LoWPAN protocol refers to IPv6 Low Power Personal Area Network which uses a lightweight IP-based communication to travel over low data rate networks. It has limited processing ability to transfer information wirelessly using an internet protocol. So, it is mainly used for home and building automation. The 6LoWPAN protocol operates only within the 2.4 GHz frequency range with 250 kbps transfer rate. It has a maximum length of 128-bit header packets.

6LowPAN Security Measure

Security is a major issue for 6LowPAN communication Protocol. There are several attacks issues at the security level of 6LoWPAN which aim is to direct destruction of the network. Since it is the combination of two systems, so, there is a possibility of attack from two sides that targets all the layer of the 6LoWPAN stack (Physical layer, Data link layer, Adaptation layer, Network layer, Transport layer, Application layer).

Properties of 6LowPAN protocol

- **Standard:** RFC6282
- **Frequency:** Used over a variety of other networking media including Bluetooth Smart (2.4GHz) or ZigBee or low-power RF (sub-1GHz)
- **Range:** NA
- **Data Rates:** NA

6TiSCH

The IETF IPv6 over the TSCH mode of IEEE802. 15.4e (6TiSCH) working group has standardized a set of protocols to enable low power industrial-grade IPv6 networks. 6TiSCH proposes a **protocol stack rooted in the Time Slotted** Channel Hopping (TSCH) mode of the IEEE802.

The Internet Engineering Task Force (IETF) has standardized a set of protocols to respond to the increasing demand for IP-enabled constrained devices. Several working groups have been created to design and develop standard specifications for devices to empower the IoT. These groups have targeted the integration of different link layer technologies to the Internet Protocol (IP) ecosystem, dealing with major limitations imposed by the underlying technologies in terms of payload size, memory footprint, computing capacity and non-trivial topologies, while ensuring IP-compliance. The IETF IPv6 over the TSCH mode of IEEE802.15.4e (6TiSCH) Working Group (WG) was created to work on the standardization of the control plane and the IP layer adaptation on top of the IEEE802.15.4 TSCH link layer . 6TiSCH has been one of the main efforts to bring IPv6 to industrial low-power wireless, bridging Time Slotted Channel Hopping (TSCH) networks with 6LoWPAN networks. This pioneering work has identified and addressed the many remaining challenges when building IPv6 on low capacity networks. It has become a glue for the different layers, and has triggered improvements in header compression, IP-in-IP encapsulation, and 6LoWPAN Neighbor Discovery, providing more capable routing schemes and security management consistently aiming at more efficiency and simplicity.

Neighbor discovery(ND) Protocol

Neighbor Discovery (ND) is a set of processes and messages. It is defined in RFC4861. It replaces ARP, ICMP Router Discovery, and the ICMP Redirect message used in IPv4. Besides replacing these functions of IPv4, it also provides a lot of additional functionalities that simplify network administration and management.

Functions of Neighbor discovery

Nodes use ND to discover each other's presence on the same link, to determine each other's link-layer addresses, to perform duplicate address detection, to discover routers serving the subnet, to automatically configure the default gateway, to discover the subnet address on which they are connected, and to maintain reachability information about the paths.

Routers use ND to advertise their presence, subnet prefixes, routes, and host configuration parameters. If a better route is available for a specific destination, routers also use this message to inform the host about it.

Neighbor Discovery message types

ND uses five different types of messages to perform all its functions. These messages are Router Advertisement, Router Solicitation, Neighbor Solicitation, Neighbor Advertisement, and Redirect. These messages are defined in RFC2461. Let's understand these messages.

Router advertisement

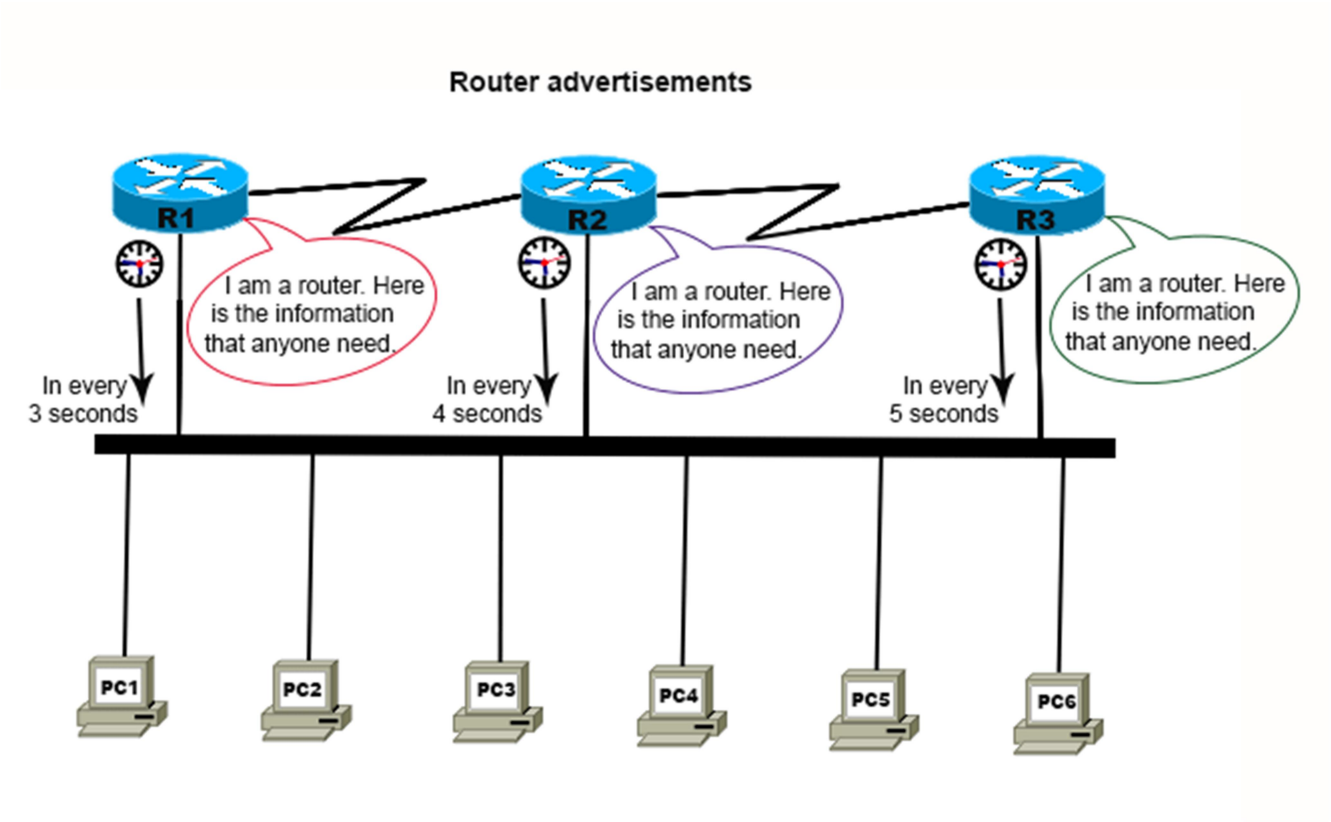
An IPv6 router uses this message to advertise its presence on the link. This message contains information that the interfaces on the links use to configure themselves. This information includes the router's IP address and link-layer address, whether this router can be used as default gateway router, subnet prefix, link MTU, specific routes, whether a DHCPv6 server is available in the network, whether an interface can configure its address through the address auto-configuration feature, and if yes the duration for which the address will be valid.

If a DHCPv6 server is available, two flags in the router advertisement are used to indicate it. These flags are the managed address configuration flag and the other configuration flag. The **M** bit and **O** bit are used to set these flags respectively. The **M** bit indicates that DHCPv6 services are available for address and configuration settings. The **O** bit indicates whether the

configuration parameters other than the IP address are available through the DHCPv6 service.

Routers send Router Advertisement messages periodically. The interval between advertisements is randomized to reduce synchronization issues when there are multiple advertising routers exist on the link.

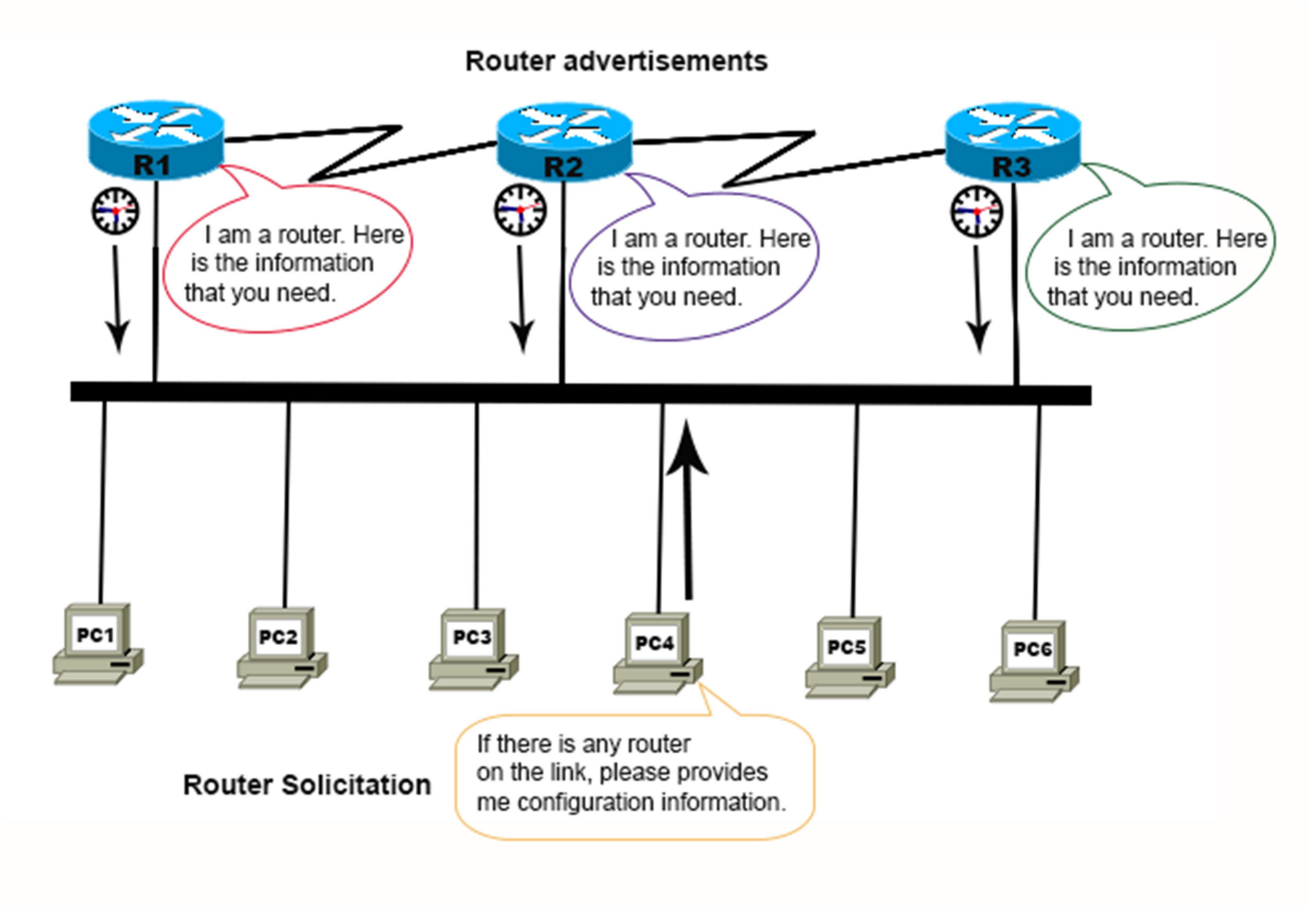
The following image shows an example of the router advertisement.



Router Solicitation

A host sends this message to request IPv6 routers on the link to generate Router Advertisements immediately rather than at their next scheduled time. When a router receives a Router Solicitation message, it responds to the message immediately. It sends a Router Advertisement to the sender host. The difference between this advertisement and the advertisements that the router sends periodically is that this advertisement is intended for a specific host only while periodic advertisements are intended for all hosts on the link.

The following image shows an example of the router solicitation.



Neighbor Solicitation

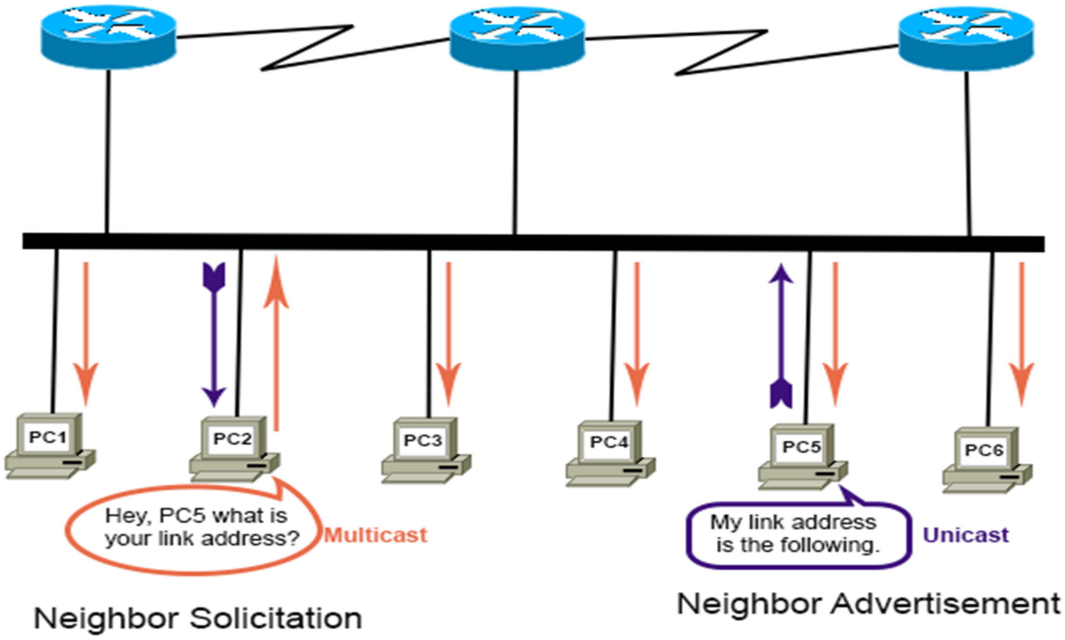
A node mainly uses this message for three purposes; to determine the link-layer address of a neighbor, to check the validity of an already determined address, and to check whether an address created through the address auto-configuration process is unique.

Since in the first purpose, the destination address is not available, the node multicasts the Neighbor Solicitation message. In the remaining two purposes, since the destination address is available, the node unicasts the Neighbor Solicitation message.

Neighbor Advertisement

A node uses this message to respond to a Neighbor Solicitation message. If a node receives a neighbor solicitation message, it sends a neighbor advertisement message back to the sender node. A node also uses this message to announce a link-layer address change. This message contains information required by nodes to determine the type of neighbor advertisement message, the link-layer address of the sender, and the sender's role on the network.

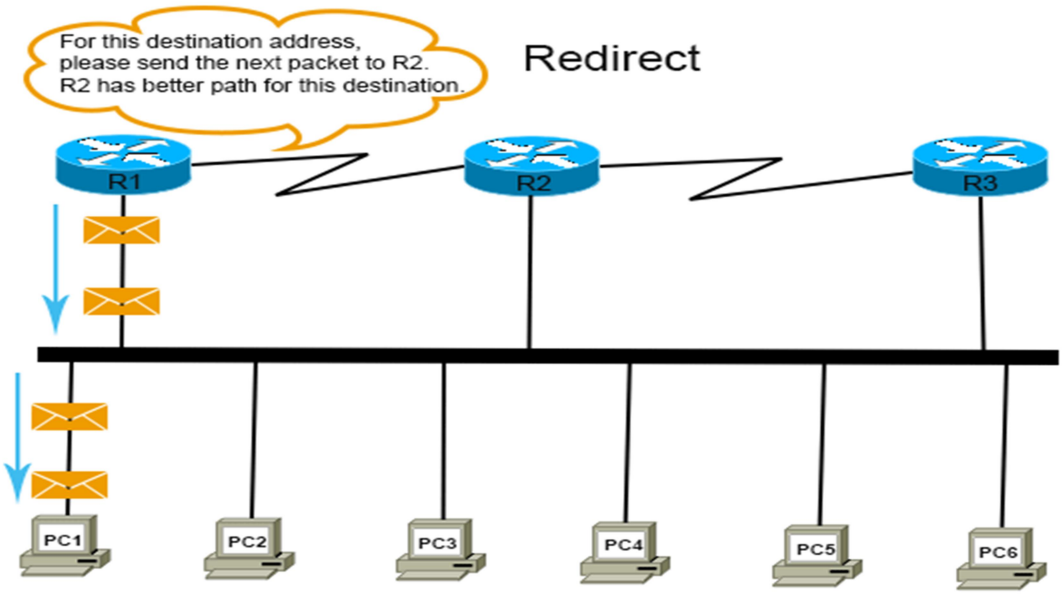
The following image shows an example of the neighbor solicitation and neighbor advertisement.



Redirect message

IPv6 routers use this message to inform an originating host about a better next-hop address for a specific destination. Only routers can send redirect messages for unicast traffic. Redirect messages are processed only by hosts.

The following image shows an example of the redirect message.



Neighbor Discovery processes

The following table summarizes the processes that use the neighbor discovery messages.

Process	***What does happen in this process?***
Router discovery	Hosts discover the routers attached on the same link.
Prefix discovery	Hosts discover the subnet or network prefixes for local link destinations.
Parameter discovery	Hosts discover additional parameters and configuration settings including the link MTU (Maximum Transmission Unit) and the default hop limit for outgoing packets.
Address auto-configuration	Interfaces configure their IP addresses either in the presence or absence of a DCHPv6 server.
Address resolution	Nodes resolve a neighbor's IPv6 address to its link-layer address.
Next-hop determination	A node determines the device to which a packet is being forwarded, based on the destination address. If the destination address is available in the local link, the next-hop address is the destination address. If the destination address is not available in the local link, the next-hop address is the address of an on-link default router.
Neighbor unreachability detection	A node determines whether a specific neighbor is still available on the on-link or has moved to a different link.
Duplicate address detection	A node determines whether an address selected by it for use is not already in use by a neighboring node.
Redirect function	A router informs a host about a better first-hop address to reach a destination.

Dynamic Host Configuration Protocol (DHCP)

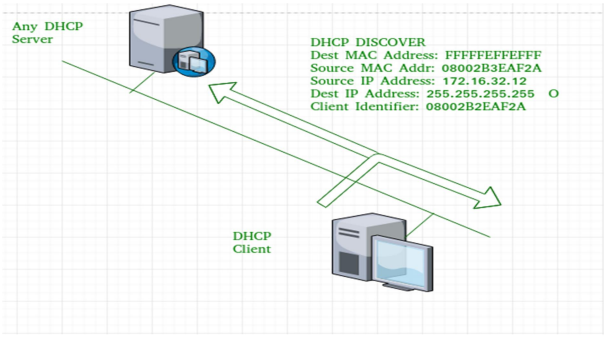
Dynamic Host Configuration Protocol(DHCP) is an application layer protocol which is used to provide:

1. Subnet Mask (Option 1 – e.g., 255.255.255.0)
2. Router Address (Option 3 – e.g., 192.168.1.1)
3. DNS Address (Option 6 – e.g., 8.8.8.8)
4. Vendor Class Identifier (Option 43 – e.g., 'unifi' = 192.168.1.9 ##where unifi = controller)

DHCP is based on a client-server model and based on discovery, offer, request, and ACK.

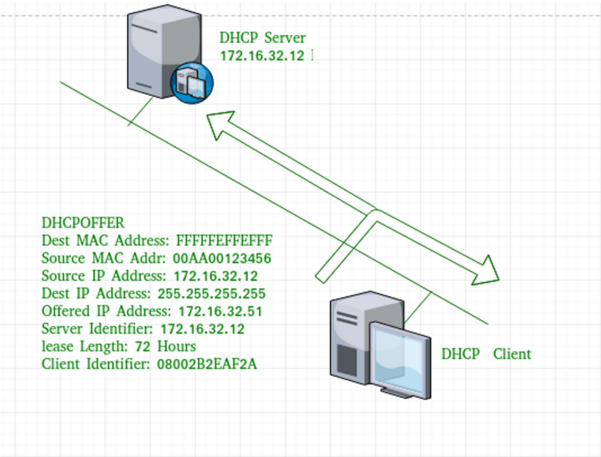
DHCP **port number** for server is 67 and for the client is 68. It is a Client server protocol which uses UDP services. IP address is assigned from a pool of addresses. In DHCP, the client and the server exchange mainly 4 DHCP messages in order to make a connection, also called DORA process, but there are 8 DHCP messages in the process.
These messages are given as below:

1. **DHCP discover message –**
   This is a first message generated in the communication process between server and client. This message is generated by Client host in order to discover if there is any DHCP server/servers are present in a network or not. This message is broadcasted to all devices present in a network to find the DHCP server. This message is 342 or 576 bytes long



   As shown in the figure, source MAC address (client PC) is 08002B2EAF2A, destination MAC address(server) is FFFFFFFFFFFF, source IP address is 0.0.0.0(because PC has no IP address till now) and destination IP address is 255.255.255.255 (IP address used for broadcasting). As the discover message is broadcast to find out the DHCP server or servers in the network therefore broadcast IP address and MAC address is used.

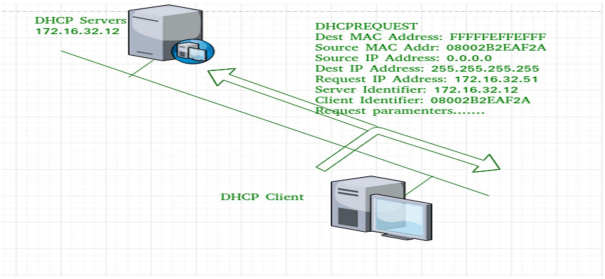
2. **DHCP offer message –**
   The server will respond to host in this message specifying the unleased IP address and other TCP configuration information. This message is broadcasted by server. Size of message is 342 bytes. If there are more than one DHCP servers present in the network then client host will accept the first DHCP OFFER message it receives. Also a server ID is specified in the packet in order to identify the server.



Now, for the offer message, source IP address is 172.16.32.12 (server's IP address in the example), destination IP address is 255.255.255.255 (broadcast IP address) ,source MAC address is 00AA00123456, destination MAC address is FFFFFFFFFFFF. Here, the offer message is broadcast by the DHCP server therefore destination IP address is broadcast IP address and destination MAC address is FFFFFFFFFFFF and the source IP address is server IP address and MAC address is server MAC address.

Also the server has provided the offered IP address 192.16.32.51 and lease time of 72 hours(after this time the entry of host will be erased from the server automatically) . Also the client identifier is PC MAC address (08002B2EAF2A) for all the messages.

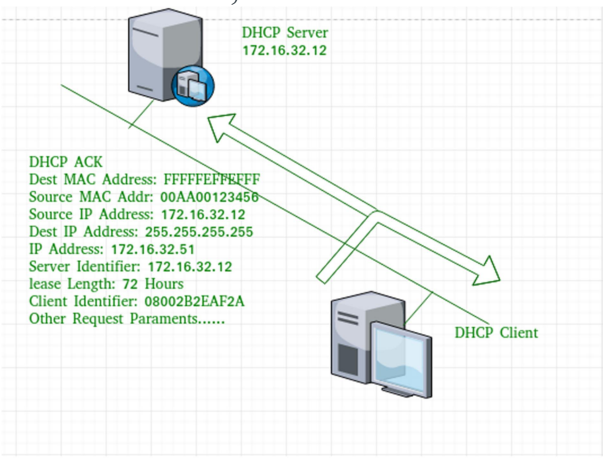
3. **DHCP request message –**
   When a client receives a offer message, it responds by broadcasting a DHCP request message. The client will produce a gratitutous ARP in order to find if there is any other host present in the network with same IP address. If there is no reply by other host, then there is no host with same TCP configuration in the network and the message is broadcasted to server showing the acceptance of IP address .A Client ID is also added in this message.



Now, the request message is broadcast by the client PC therefore source IP address is 0.0.0.0(as the client has no IP right now) and destination IP address is 255.255.255.255 (broadcast IP address) and source MAC address is 08002B2EAF2A (PC MAC address) and destination MAC address is FFFFFFFFFFFF.

Note – This message is broadcast after the ARP request broadcast by the PC to find out whether any other host is not using that offered IP. If there is no reply, then the client host broadcast the DHCP request message for the server showing the acceptance of IP address and Other TCP/IP Configuration.

4. **DHCP acknowledgement message –**
   In response to the request message received, the server will make an entry with specified client ID and bind the IP address offered with lease time. Now, the client will have the IP address provided by server.



Now the server will make an entry of the client host with the offered IP address and lease time. This IP address will not be provided by server to any other host. The destination MAC address is FFFFFFFFFFFF and the destination IP address is 255.255.255.255 and the source IP address is 172.16.32.12 and the source MAC address is 00AA00123456 (server MAC address).

5. **DHCP negative acknowledgement message –**
   Whenever a DHCP server receives a request for IP address that is invalid according to the scopes that is configured with, it send DHCP

Nak message to client. Eg-when the server has no IP address unused or the pool is empty, then this message is sent by the server to client.

6. **DHCP decline –**
   If DHCP client determines the offered configuration parameters are different or invalid, it sends DHCP decline message to the server .When there is a reply to the gratuitous ARP by any host to the client, the client sends DHCP decline message to the server showing the offered IP address is already in use.
7. **DHCP release –**
   A DHCP client sends DHCP release packet to server to release IP address and cancel any remaining lease time.
8. **DHCP inform –**
   If a client address has obtained IP address manually then the client uses a DHCP inform to obtain other local configuration parameters, such as domain name. In reply to the dhcp inform message, DHCP server generates DHCP ack message with local configuration suitable for the client without allocating a new IP address. This DHCP ack message is unicast to the client.

Note – All the messages can be unicast also by dhcp relay agent if the server is present in different network.

Advantages – The advantages of using DHCP include:

- centralized management of IP addresses
- ease of adding new clients to a network
- reuse of IP addresses reducing the total number of IP addresses that are required
- simple reconfiguration of the IP address space on the DHCP server without needing to reconfigure each client

The DHCP protocol gives the network administrator a method to configure the network from a centralised area.

With the help of DHCP, easy handling of new users and reuse of IP address can be achieved.

Disadvantages – Disadvantage of using DHCP is:

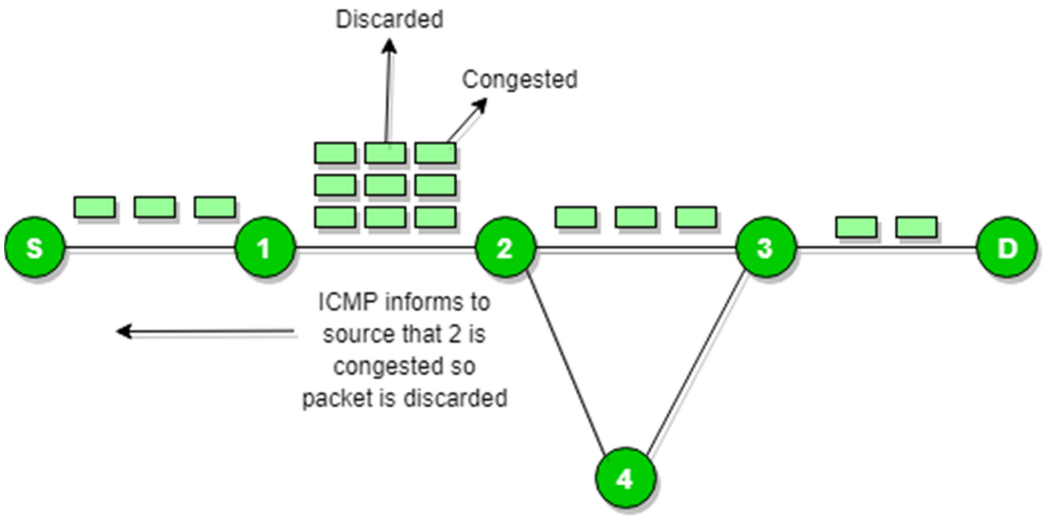
- IP conflict can occur

ICMP Protocol

Since IP does not have an inbuilt mechanism for sending error and control messages. It depends on Internet Control Message Protocol(ICMP) to provide an error control. It is used for reporting errors and management queries. It is a supporting protocol and is used by networks devices like routers for sending error messages and operations information.
e.g. the requested service is not available or that a host or router could not be reached.

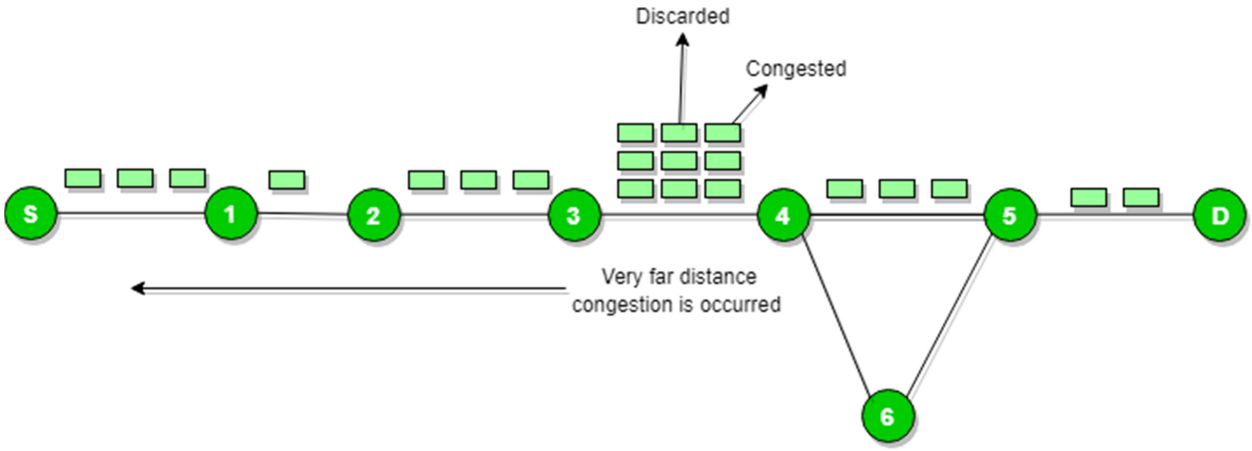
Source quench message :

Source quench message is a request to decrease the traffic rate for messages sending to the host(destination). Or we can say when receiving host detects that the rate of sending packets (traffic rate) to it is too fast it sends the source quench message to the source to slow the pace down so that no packet can be lost.



ICMP will take the source IP from the discarded packet and informs the source by sending a source quench message.

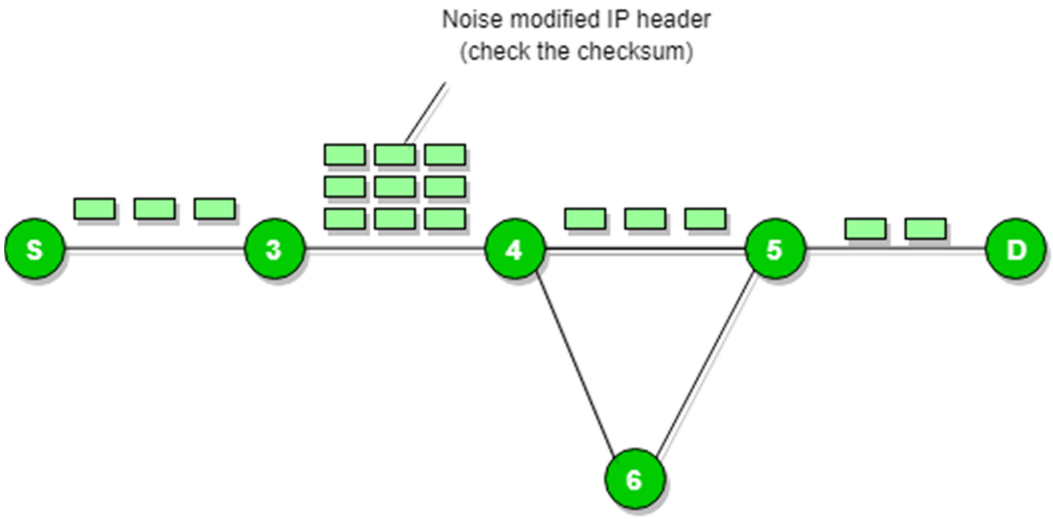
Then source will reduce the speed of transmission so that router will be free from congestion.



When the congestion router is far away from the source the ICMP will send hop by hop source quench message so that every router will reduce the speed of transmission.

Parameter problem :

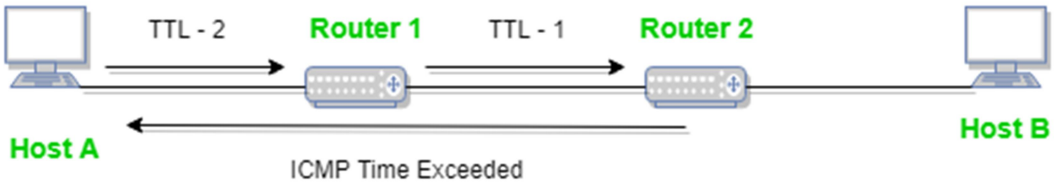
Whenever packets come to the router then the calculated header checksum should be equal to the received header checksum then the only the packet is accepted by the router.

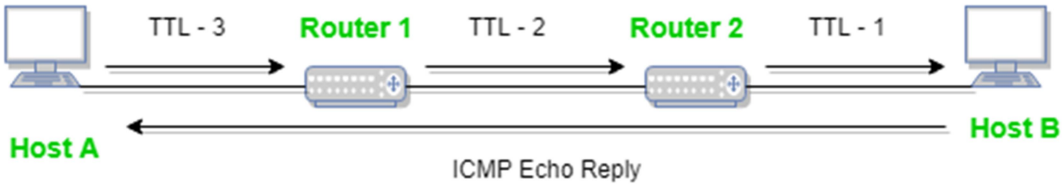


If there is a mismatch packet will be dropped by the router.

ICMP will take the source IP from the discarded packet and informs to the source by sending a parameter problem message.

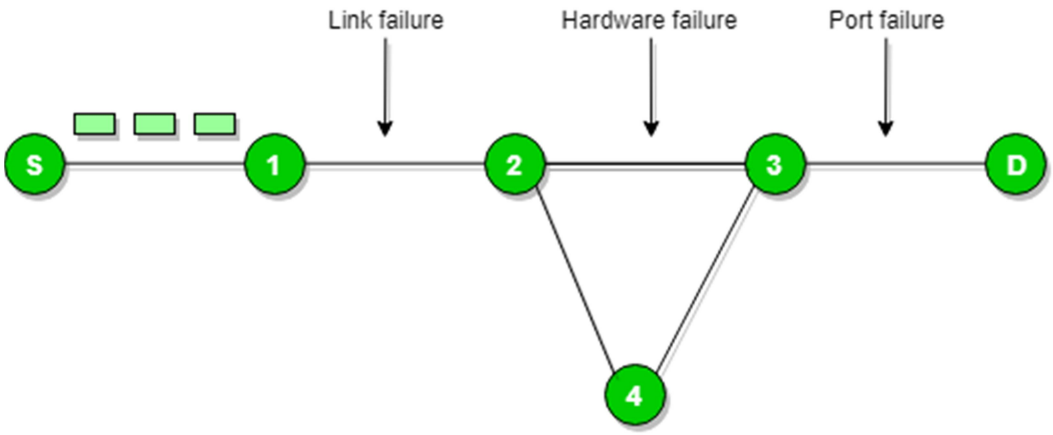
Time exceeded message :





When some fragments are lost in a network then the holding fragment by the router will be dropped then ICMP will take the source IP from the discarded packet and informs the source, of discarded datagram due to time to live field reaches zero, by sending time exceeded message.

Destination un-reachable :
Destination unreachable is generated by the host or its inbound gateway to inform the client that the destination is unreachable for some reason.



There is no necessary condition that the only the router gives the ICMP error message some time the destination host sends an ICMP error message when

any type of failure (link failure, hardware failure, port failure, etc) happens in the network.

Redirection message :
Redirect requests data packets are sent on an alternate route. The message informs a host to update its routing information (to send packets on an alternate route).

Ex. If the host tries to send data through a router R1 and R1 sends data on a router R2 and there is a direct way from the host to R2. Then R1 will send a redirect message to inform the host that there is the best way to the destination directly through R2 available. The host then sends data packets for the destination directly to R2.
The router R2 will send the original datagram to the intended destination.
But if the datagram contains routing information then this message will not be sent even if a better route is available as redirects should only be sent by gateways and should not be sent by Internet hosts.

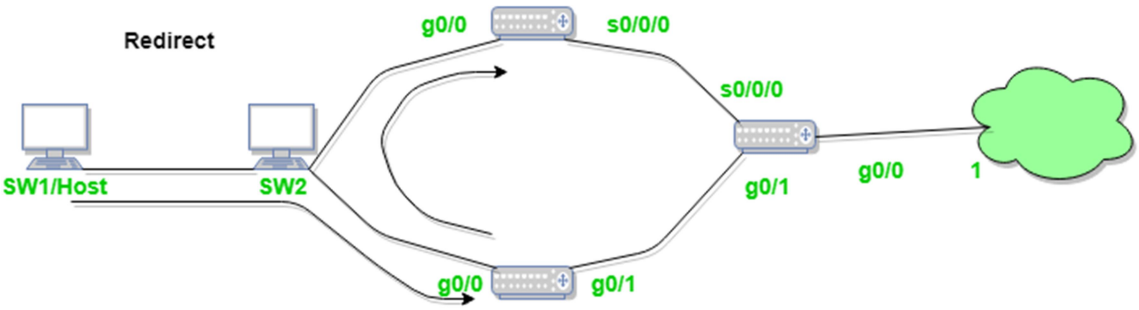


Figure - ICMP redirect Verification CCNP 2.0 100 - 101 (v - 71)

- ICMP Redirect
- ICMP Redirect for host
- ICMP Redirect for network
- How ICMP redirect work
- ICMP Redirect verification step by step

Whenever a packet is forwarded in a wrong direction later it is re-directed in a current direction then ICMP will send a re-directed message.

RPL Protocol

RPL is an IPv6 routing protocol that is standardized for the Internet of Things (IoT) by Internet-Engineering Task Force (IETF). RPL forms a tree-like topology which is based on different optimizing process called Objective Function (OF).

RPL stands for *Routing Protocol for Low-Power and Lossy Network*. It is a distance-vector protocol that supports a varity of Data Link Protocols. RPL builds a **Destination Oriented Directed Acyclic Graph (DODAG)** which has only one route from each leaf node to the root. All the traffic in this DODAG is routed through the root. Initially, each node sends a DODAG Information Object (DIO) announcing them self as a root. This information travels in the network, and complete DODAG is gradually built. When a new node wants to join the network, it sends a DODAG Information Solicitation (DIS) request and root responds back with a DAO Acknowledgment (DAO-ACK) confirming the join.

RPL is designed to **support Home, Building, Smart Grid and Smart Cities networks**. Thus, the routing protocol must support from a few dozens to a few thousands of nodes in a single LLN.

CORPL Protocol

CORPL protocol is the extension of the **RPL protocol**, which is termed as **cognitive RPL**. This network protocol is designed for cognitive networks and uses DODAG topology. CORPL protocol makes two new modifications in the RPL protocol. It uses opportunistic forwarding to forward a packet between the nodes. Each node of CORPL protocol keeps the information of forwarding set rather than parents only maintaining it. Each node updates its changes to its neighbour using DIO messages. On the basis of this updated message, each node frequently updates its neighbour for constant forwarder set.

CARP Protocol

CARP (Channel-Aware Routing Protocol) is a distributed routing protocol. It is designed for underwater communication. It has lightweight packets so that it can be used for Internet of Things (IoT). It performs two different functionalities: network initialization and data forwarding. CARP protocol does not support previously collected data. Hence, it is not beneficial for those IoT or other application where data is changed frequently. The up-gradation of CARP is done in E-CARP which overcomes the limitation of CARP. The E-CARP allows the sink node to save previously received sensory data.