**Assignment 2**

**M.K.H.S. Gujarati Girls College, Indore**

**Name : Aayushi Sethi**

**Class : BCA V sem**

**Subject : Computer Networks**

**Q.1. What is router ? Explain how it works.**

**Ans.** A router is a device that communicates between the internet and the devices in your home that connect to the internet. As its name implies, it “routes” traffic between the devices and the internet.

Router connect computers and other devices to the Internet. A router acts as a dispatcher, choosing the best route for your information to travel. It connects your business to the world, protects information from security threats, and can even decide which computers get priority over others.

A typical home has a range of internet-connected devices — personal computers, tablets, smartphones, printers, thermostats, smart TVs, and more. With your router, these devices form a network. A router directs incoming and outgoing internet traffic on that network in the fastest and most efficient way.

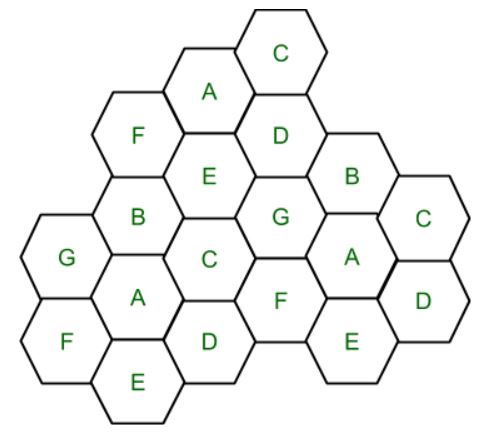
The information traveling on your home network could be an email, a movie, or a live feed from your baby cam, each of which takes up varying amounts of bandwidth. Making sure that information is delivered quickly and correctly is a big task — and getting bigger. As you add more and more devices — think [Internet of Things](https://us.norton.com/internetsecurity-iot-what-is-the-internet-of-things.html) — you ask your router to do more.

**Q.2. What is frequency reuse.**

**Ans.** Technique for using a specified range of frequencies more than once in the same radio system so that the total capacity of the system is increased without increasing its allocated bandwidth. Frequency reuse schemes require sufficient isolation among the signals that use the same frequencies so that mutual interference among them is controlled at an acceptable level. For satellites, frequency reuse can be achieved by using orthogonal polarization states for transmission and/or by using satellite antenna (spot) beams that serve separate, non-overlapping geographic regions.

**Frequency Reuse** is the scheme in which allocation and reuse of channels throughout a coverage region is done. Each cellular base station is allocated a group of radio channels or Frequency sub-bands to be used within a small geographic area known as a cell. The shape of the cell is Hexagonal. The process of selecting and allocating the frequency sub-bands for all of the cellular base station within a system is called **Frequency reuse** or **Frequency Planning**.

**Silent Features of using Frequency Reuse:**

* Frequency reuse improve the spectral efficiency and signal Quality (QoS).
* Frequency reuse classical scheme proposed for GSM systems offers a protection against interference.
* The number of times a frequency can be reused is depend on the tolerance capacity of the radio channel from the nearby transmitter that is using the same frequencies.
* In Frequency Reuse scheme, total bandwidth is divided into different sub-bands that are used by cells
* . Frequency reuse scheme allow WiMax system operators to reuse the same frequencies at different cell sites.
* 

**Q.3. What is IPV4 and IPV6. Differentiate both.**

**Ans.**

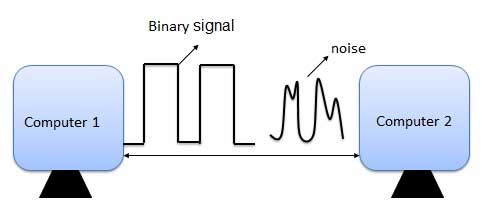
**IPV4** and **[IPv6](https://www.geeksforgeeks.org/internet-protocol-v6-ipv6/" \t "https://www.geeksforgeeks.org/differences-between-ipv4-and-ipv6/_blank)**are internet protocol version 4 and internet protocol version 6, IP version 6 is the new version of Internet Protocol, which is way better than IP version 4 in terms of complexity and efficiency.

**Difference Between IPv4 and IPv6:**

|  |  |
| --- | --- |
| ****IPV4**** | ****IPV6**** |
| IPv4 has 32-bit address length | IPv6 has 128-bit address length |
| It Supports Manual and DHCP address configuration | It supports Auto and renumbering address configuration |
| In IPv4 end to end connection integrity is Unachievable | In IPv6 end to end connection integrity is Achievable |
| It can generate 4.29×109 address space | Address space of IPv6 is quite large it can produce 3.4×1038 address space |
| Security feature is dependent on application | IPSEC is inbuilt security feature in the IPv6 protocol |
| Address representation of IPv4 is in decimal | Address Representation of IPv6 is in hexadecimal |
| Fragmentation performed by Sender and forwarding routers | In IPv6 fragmentation performed only by sender |
| In IPv4 Packet flow identification is not available | In IPv6 packetflow identification are Available and uses flow label field in the header |
| In IPv4 checksumfield is available | In IPv6 checksumfield is not available |
| It has broadcast Message Transmission Scheme | In IPv6 multicast and any cast message transmission scheme is available |
| In IPv4 Encryption and Authentication facility not provided | In IPv6 Encryption and Authentication are provided |
| IPv4 has header of 20-60 bytes | IPv6 has header of 40 bytes fixed |

**Q.5. What is error detection and correction ? How to check it on parity checker ?**

**Ans.** Error is a condition when the output information does not match with the input information. During transmission, digital signals suffer from noise that can introduce errors in the binary bits travelling from one system to other. That means a 0 bit may change to 1 or a 1 bit may change to 0.



## Error-Detecting codes

Whenever a message is transmitted, it may get scrambled by noise or data may get corrupted. To avoid this, we use error-detecting codes which are additional data added to a given digital message to help us detect if an error occurred during transmission of the message. A simple example of error-detecting code is **parity check**.

## Error-Correcting codes

Along with error-detecting code, we can also pass some data to figure out the original message from the corrupt message that we received. This type of code is called an error-correcting code. Error-correcting codes also deploy the same strategy as error-detecting codes but additionally, such codes also detect the exact location of the corrupt bit.

In error-correcting codes, parity check has a simple way to detect errors along with a sophisticated mechanism to determine the corrupt bit location. Once the corrupt bit is located, its value is reverted (from 0 to 1 or 1 to 0) to get the original message.

## Detect and Correct Errors?

* + To detect and correct the errors, additional bits are added to the data bits at the time of transmission.
  + The additional bits are called **parity bits**. They allow detection or correction of the errors.
  + The data bits along with the parity bits form a **code word**.

## Parity Checking of Error Detection

It is the simplest technique for detecting and correcting errors. The MSB of an 8-bits word is used as the parity bit and the remaining 7 bits are used as data or message bits. The parity of 8-bits transmitted word can be either even parity or odd parity.

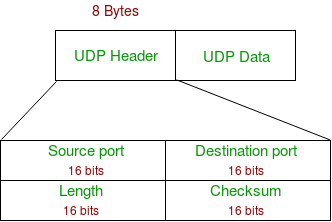
**Q.6. Explain UDP network security ?**

**Ans. User Datagram Protocol (UDP)** is a Transport Layer protocol. UDP is a part of Internet Protocol suite, referred as UDP/IP suite. Unlike TCP, it is **unreliable and connectionless protocol.** So, there is no need to establish connection prior to data transfer.

Though Transmission Control Protocol (TCP) is the dominant transport layer protocol used with most of Internet services; provides assured delivery, reliability and much more but all these services cost us with additional overhead and latency. Here, UDP comes into picture. For the realtime services like computer gaming, voice or video communication, live conferences; we need UDP. Since high performance is needed, UDP permits packets to be dropped instead of processing delayed packets. There is no error checking in UDP, so it also save bandwidth.

**UDP Header –**

UDP header is **8-bytes** fixed and simple header, while for TCP it may vary from 20 bytes to 60 bytes. First 8 Bytes contains all necessary header information and remaining part consist of data. UDP port number fields are each 16 bits long, therefore range for port numbers defined from 0 to 65535; port number 0 is reserved. Port numbers help to distinguish different user requests or process.



1. **Source Port :** Source Port is 2 Byte long field used to identify port number of source.
2. **Destination Port :** It is 2 Byte long field, used to identify the port of destined packet.
3. **Length :** Length is the length of UDP including header and the data. It is 16-bits field.
4. **Checksum :** Checksum is 2 Bytes long field. It is the 16-bit one’s complement of the one’s complement sum of the UDP header, pseudo header of information from the IP header and the data, padded with zero octets at the end (if necessary) to make a multiple of two octets.

**Notes –** Unlike TCP, Checksum calculation is not mandatory in UDP. No Error control or flow control is provided by UDP. Hence UDP depends on IP and ICMP for error reporting.

**Applications of UDP:**

* Used for simple request response communication when size of data is less and hence there Is lesser concern about flow and error control.
* It is suitable protocol for multicasting as UDP supports packet switching.
* UDP is used for some routing update protocols like RIP(Routing Information Protocol).
* Normally used for real time applications which can not tolerate uneven delays between sections of a received message.
* Following implementations uses UDP as a transport layer protocol:
  + NTP (Network Time Protocol)
  + DNS (Domain Name Service)
  + BOOTP, DHCP.
  + NNP (Network News Protocol)
  + Quote of the day protocol
  + TFTP, RTSP, RIP.
* Application layer can do some of the tasks through UDP-
  + Trace Route
  + Record Route
  + Time stamp
* UDP takes datagram from Network Layer, attach its header and send it to the user. So, it works fast.
* Actually UDP is null protocol if you remove checksum field.
  1. Reduce the requirement of computer resources.
  2. When using the Multicast or Broadcast to transfer.
  3. The transmission of Real-time packets, mainly in multimedia applications.