

**An Assignment of**

**Computer Networks :CSE306**

****

**Name : Simran Manhas**

**Registration Number :** 11803523

**Section :** K18HA

**Submitted to : Harjit Singh Sir(14952)**

**SET-A**

**Question 1**

**Q1.**

**1.1.Answer:**

**1.2.Answer:**

As we know that the simple parity check technique is a process of transferring data from one node to another during any exchange of data accurately.

Since during transmission or exchange of data there may be some limitations of simple parity check. There are following limitations of parity bit check:

**A)Corruption in Parity Bit:-**

Corruption in parity bit can be considered as major drawback because when any data transferred and if there is any corruption in parity bits then receiver discard whole valid data. This cause loss of data while exchange of data.

1. **Corruption in Data Bit:-**

Sometimes while transferring data, some bits of data get corrupted and leave the binary 1’s as same as before but change the data value.This type of corruption in data bit leads to corruption of whole data but receiver still get data without any loss and the data do not get detected by receiving station as parity bits get matched after corruption.

**C)Combination of Both the corruption:-**

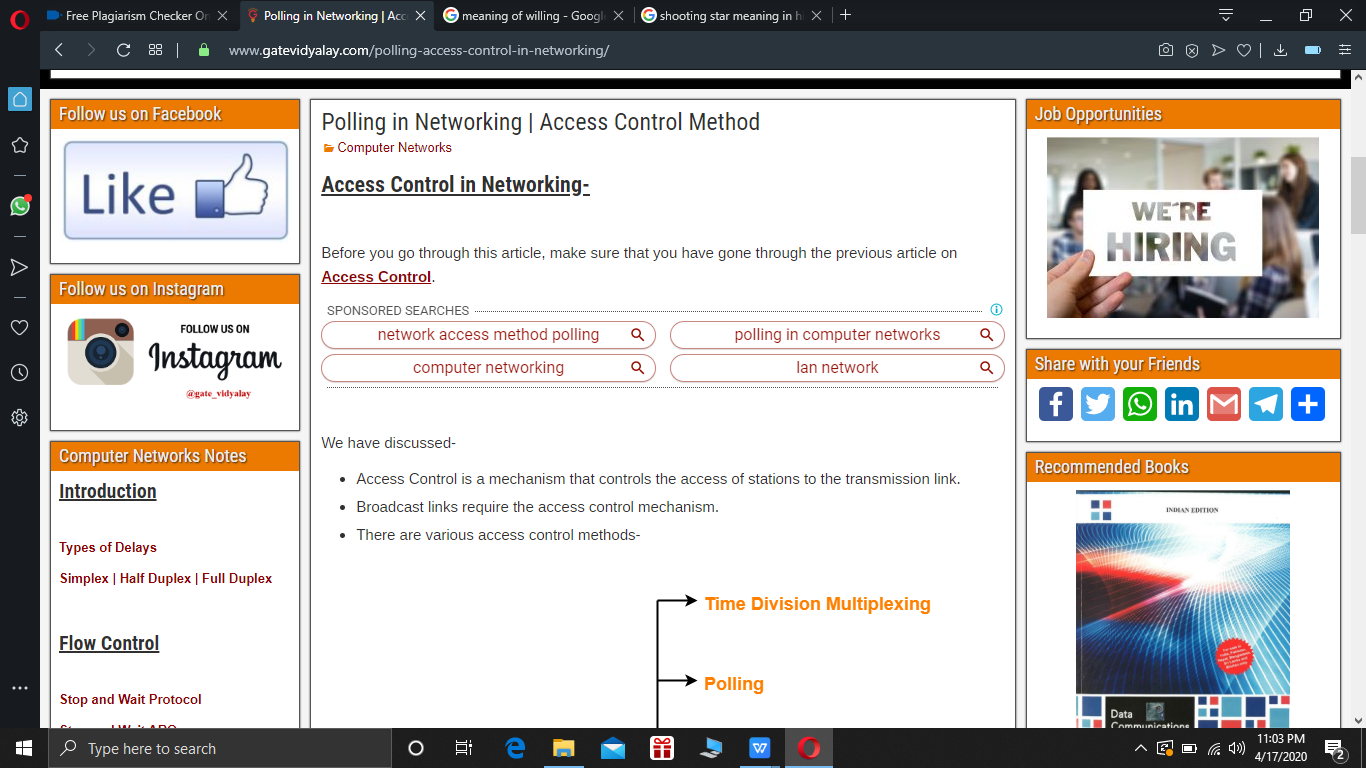
In some cases there are corruption in both parity as well as data bits but somehow they get matched. After matching of them receiver accept the data but ultimately it get corrupted.

**1.3.Answer:**

**We can select a device through the following concept:**

The transmission of data is done by means of some type of transmission media to transmit data from one computer to another. The sharing of knowledge between two machines by some sort of media, such as the cable. Networking systems must be part of a communication infrastructure consisting of a variety of equipment (physical equipment) and computer-based applications (programs) for data transmission purposes. Information transmission is the electronic processing mechanism of a interactive data transfer amongst several or even more machines. A telecom network allows the exchanging of electronic between machines.

**1.4.Answer:**



The technique used to control station access to an interchange communication connection.

Poll feature generally referred as polling, it is a form of managed method of access that controls a survey or polling where all the terminals are ready to move data.

Let's see how a polling func actually works:

A)Polling is usually accessed or managed by a primary tool that asks for a transmission of data from other devices.

B)After asking for data exchange , the request by poll function is done to poll another stations when the primary device get ready to receive whether any station wants to transfer data or not.

C)Once the primary system gets ready to receive whether or not another station wants to move data, the polling feature demands that another station be compromised after requesting data exchange.

D)Secondary system will respond either with NAK after polling if it does not send any data or if it does.

E) Once a device get negative response which means NAK frame from other devices then it will go for other devices to poll for transmission of data.

F)Lastly when it get a +ve response then it will give feedback with ACK frame (Acknowledgement).

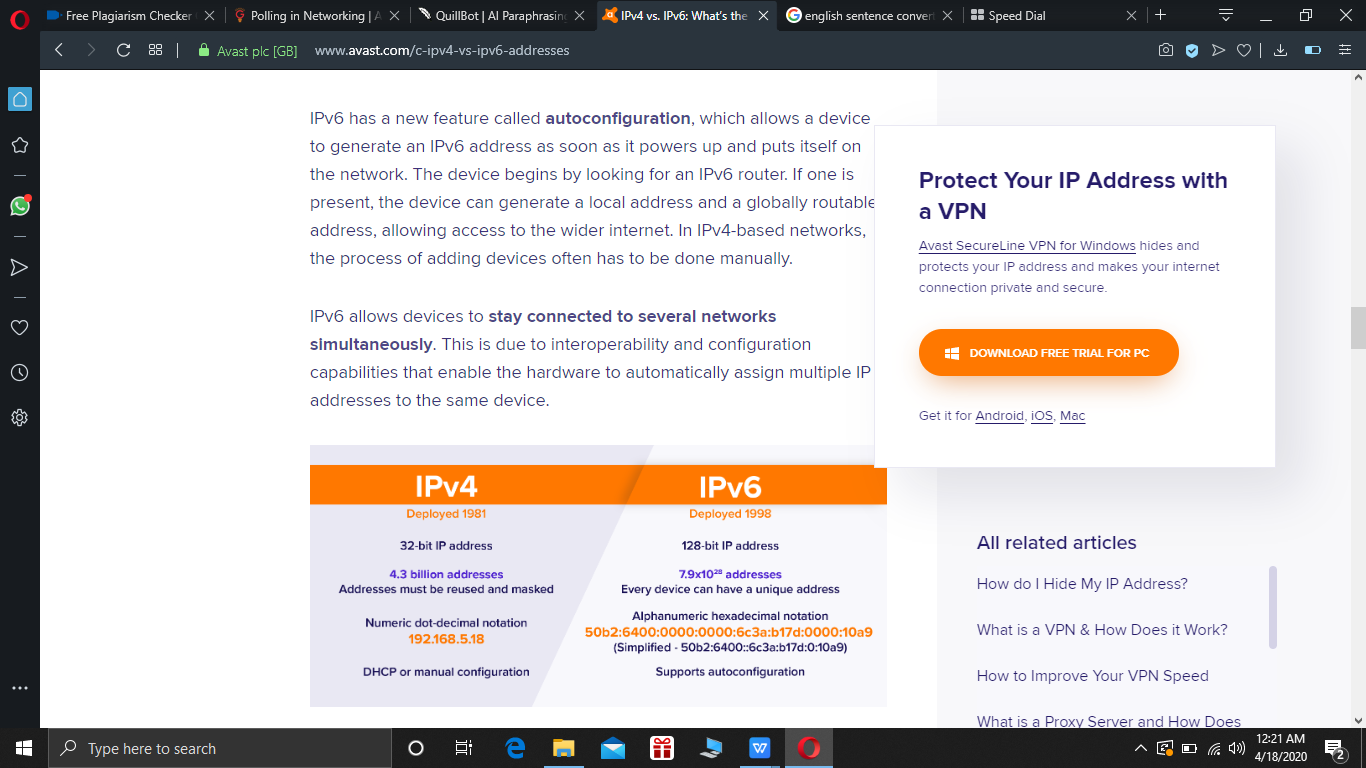
**Question 2**

**2.1.Answer:**

IPv6 can be considered as the next edition IP. IP address format implemented to complement and ultimately succeed IPv4, is still used by several Internet service facility providers today. Each smartphone, cell phone, smart home feature, Internet of Things sensor, and every other internet-connected system requires a numerical IP address to connect with each other. The IP address system initially called IPv4,is losing off of address from emergence of too many linked systems leading to its extensive utilization.

IPv6 (edition VI of the IP) has been the 6th update of the IP as well as a heir of IPv4. This works similar like IPv4 except that it provides with specific Addresses required to communicate among web-enabled devices. It has some 1 key difference though: it uses an IP address of 128bit.

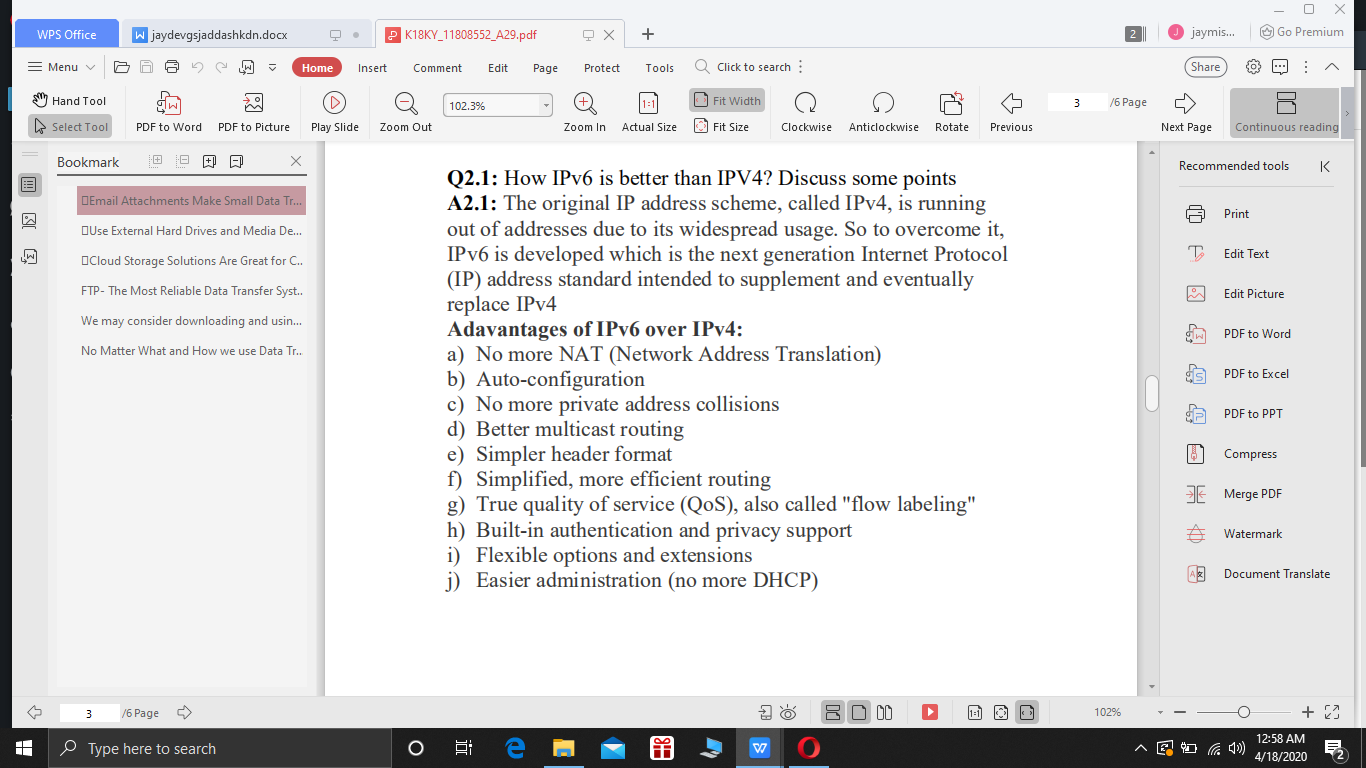
In contrast towards more IP addresses the introduction of IPv6 gave added features. For eg, IPv6 facilitates multicast addressing, that permits for the continuous transfer of latency-intensive packets streams (like media channels) to various destinations, minimizing bandwidth utilization.



In principle, IPv6 would have been a little quicker because phases of NAT transformations wouldn't have to be lost. Yet for some use cases, IPv6 often has bigger packets, which may make it quicker. What also makes a difference at this stage is that IPv4 networks are more advanced than IPv6 networks, and therefore highly engineered. But IPv6 networks can get faster with time and tuning.

With more reliability in view IPv6 has been founded. Internet Public safety (IPSec) has always been a set of safety, encryption, including quality IETF security procedures, which is completely implemented into IPv6. Another truth remains, IPSec can indeed be completely incorporated into IPv4, too. Introducing this is open for ISPs — but not every organization does.

IPv6 requires a valid authentication code — partly a cryptographic functions scheme, and another a private key —  obligated towards an add of IPv6 . A subsequent Cryptographically Created add. enables any individual to show "evidence of possession" and verify the identification for quite an unique IPv6 add..a Such functionality can not be upgraded to IPv4 with default address of 32-bit.



**2.2 Answer:**

**2.3 Answer:**

Anycast may be used as intuitive interface for routing tables in IPv6. Someone activates a router server upgrade for a network with hosts, transferring the data to the closest host. A host therefore transfers the request to its closest routers before any of the group's routing tables get modified.

**2.4 Answer:**

BGP can be preferred over the following ways  :

1. When someone is a  ISP, it is almost a necessity to operate BGP with their network. ·
2. No need to install BGP somewhere in a network through the Layer 3 VAN infrastructure because one can choose to implement MPLS / VPN approaches.
3. Deploying BGP on a Provider Edge (PE) routers to link a VPN clients and even on a several key nodes which function like routing servers is more than enough.
4. The   design of BGP depends  on some other quicker RP(routing protocol) which can provide network routing, with BGP in charge of edge / customer routing.
5. It allow us to  mention  any Logical address as an IP pre other-hop.
6. BGP has a variety of features that identify IP routes, enabling you to apply additional luggage on every IP route branded as BGP communities.

**Question -3**

**3.1. Answer:**

**Urgent Pointer:**

1. It  may be used to define priority for the method.

2. The Urgent Pointer header transmits the current value as a + ve offset from the Segment Number Series

3.If and only when the URG Flag is set is then true.

4. It may point to the Sequence Numbers of the end octet in a series which is a set of urgent results.

5.Data that is critical will be forthwith.

**Urgent Flag:**

The data which is Urgent must be submitted to the client directly to the wire from sending side and on receipient end. Because telnet is connecting to such a remote device we want to be able to execute the commands we type right after we have typed them. therefore they’re marked with urg pin.

**3.2. Answer:**

**3.3. Answer:**

TCP interface synchronisation by utilising a 3-way protocol (TCP) system must be synchronised before transmitting machine and recipient initiate the data sharing.

SYN: That had to activate and bind. Also aids in the synchronization of series numbers among computers.

ACK: Helps prove it has obtained the SYN on the other leg.

SYN-ACK: Local system SYN notification and earlier packet ACK response.

FIN: End the connection.

**3.4.Answer:**

I guess we would prefer TCP: TCP immediately allows you the power of latency, such that your code usually behaves as a "normal guy" on the network. Not UDP. UDP. TCP maintains data supply in-command. If you send A before B, you will obtain A before B from your receiver. No such assurances are given by UDP. TCP transmits information into an infinite stream so you can decide the data chunks appropriately, while UDP sends data into chunks (datagrams). You don't have to think about datum boundaries, but the datagram size is small. TCP is lent since the connection (stream socket) between all devices is carefully transmitted so that the data is received,there is also a datagram limit set, though. TCP is sluggish as there is a link between the two systems because the data is properly transferred such that all is received.