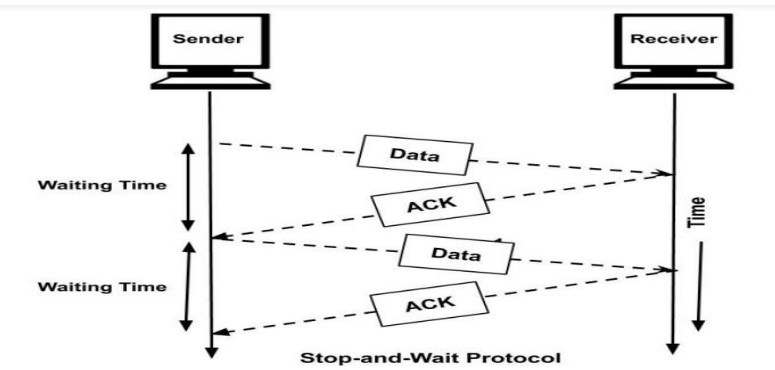
Q 1: a) Explain the "Stop and Wait" protocol? Also explain the following in brief.

ANS.

This is the simplest method of flow control. In this way, the sender will send one frame to the receiver at a time. The sender will stop and wait for the receiver's confirmation. This time (that is, the time from sending a message to receiving an acknowledgment) is the waiting time of the sender, during which the sender is completely inactive. When the sender receives an acknowledgment (ACK), it sends the next data packet to the receiver and waits for the confirmation again. As long as the sender has data to send, the process will continue. The following figure can understand this:



The figure above illustrates the normal operation in the stop and wait protocol. Now, we will see some cases of missing data or confirmation, and how to stop waiting for the protocol to respond to it.

Its background

Stop and Standby ARQ, also known as Spare Bit Protocol, is a method used in telecommunications to send information between two connected devices. It ensures that information will not be lost due to missing data packets and that the data packets are received in the correct order. This is the simplest automatic repeat request (ARQ) mechanism. Stop waiting for the ARQ transmitter to send one frame at a time; this is a special case of the general sliding window protocol, and the size of the sending and receiving windows is equal to one in both cases. After sending each frame, the sender does not send other frames until it receives an acknowledgement signal (ACK). After receiving a valid frame, the receiver sends an ACK. If the ACK does not reach the sender within a certain period of time, which is called a timeout, the sender will send the same frame again. After each frame transmission, the delay countdown is reset. The above behavior is a basic example of stopping and waiting. However, the actual implementation is different to solve some design problems.

How this protocol works?

The working of a stop and wait protocol may be explained as-

Sender sends a data packet to the receiver.

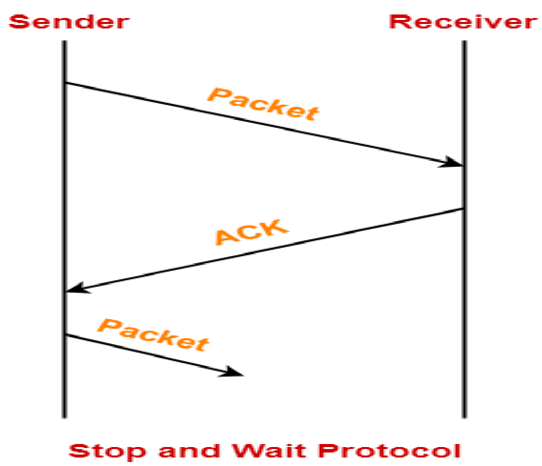
Sender stops and waits for the acknowledgement for the sent packet from the receiver.

Receiver receives and processes the data packet.

Receiver sends an acknowledgement to the sender.

After receiving the acknowledgement, sender sends the next data packet to the receiver.

These steps are illustrated below-



Shortcomings

Stop and Wait protocol. disadvantages of stop-and-wait: fairly slow: the sender can send at most one new packet per RTT. not robust: if the ack can get lost, when the receiver gets a packet, the receiver cannot tell if it is a retransmission or a new packet

It works fine only for noiseless channels.

It works on assumption that there is no delay in the network which is mostly in applicable.

It considers queying delay to be 0,which is not true in case of internet .

Transmission of packet using this protocol is very slow .

If any how the acknowledgement is not recieved by the sender it will keep waiting for long time.

It is not useful for wide area network

b) Thoroughly explain the concept of Sliding Window with its working principle? Also give an example.

ANS.

The sliding window protocol is a data link layer protocol for reliable sequential transmission of data frames. Sliding windows are also used in "Transmission Control Protocol". In this protocol, the sender can send multiple frames at once before receiving an acknowledgement from the receiver. The term sliding window refers to an imaginary box containing a frame. The sliding window method is also called windowing.

Working Principle

In these protocols, the sender has a buffer called the send window, and the receiver has a buffer called the receive window.

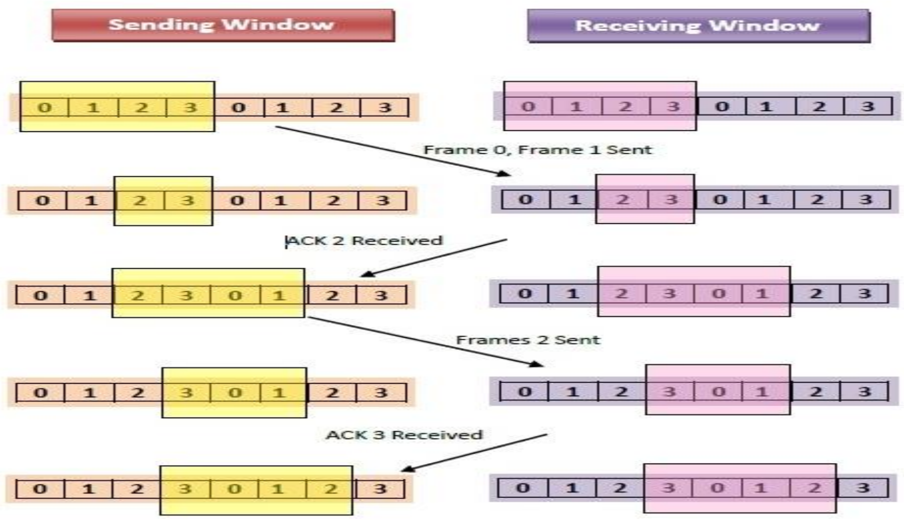
The size of the sending window determines the sequence number of the outgoing frame. If the sequence number of the frame is an n-bit field, the range of sequence numbers that can be allocated is 0 to 2 -1. Therefore, the size of the sending window is $2n$-1. Therefore, in order to adapt to the sending window size of 2π-1, an n-bit sequence number is selected.

The serial number is modulo n. For example, if the size of the sending window is 4, the sequence number will be 0, 1, 2, 3, 0, 1, 2, 3, 0, 1, etc. The number of digits in the serial number is 2 to generate the binary sequence 00, 01, 10, 11.

The size of the receiving window is the maximum number of frames that the receiver can accept at one time. It determines the maximum number of frames that the sender can send before receiving an acknowledgement.

Example

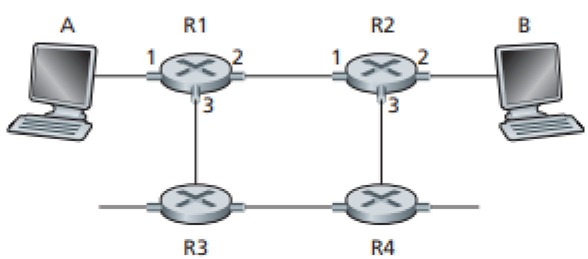
Suppose we have a transmitter window and a receiver window, and the size of each window is 4. Therefore, the sequential numbers of the two windows will be 0, 1, 2, 3, 0, 1, 2, and so on. The following figure shows the position of the window after sending the frame and receiving the confirmation.



<u>c) Why there is a need of Virtual Circuit Switching (VCS). Explain it diagrammatically.</u>

ANS.

Packets are delivered in order, since they all take the same route; The overhead in the packets is smaller, since there is no need for each packet to contain the full address; The connection is more reliable, network resources are allocated at call setup so that even during times of congestion, provided that a call has been setup, the subsequent packets should get through; Billing is easier, since billing records need only be generated per call and not per packet. Whenever a new VC is established across a router, an entry is added to the forwarding table. Similarly, whenever a VC terminates, the appropriate entries in each table along its path are removed. You might be wondering why a packet doesn't just keep the same VC number on each of the links along its route. The answer is twofold. First, replacing the number from link to link reduces the length of the VC field in the packet header. Second, and more importantly, VC setup is considerably simplified by permitting a different VC number at each link along the path of the VC. Specifically, with multiple VC numbers, each link in the path can choose a VC number independently of the VC numbers chosen at other links along the path. If a common VC number were required for all links along the path, the routers would have to exchange and process a substantial number of messages to agree on a common VC number (e.g., one that is not being used by any other existing VC at these routers) to be used for a connection.



Q 2: a) Distinguish between a root bridge and a non-root bridge.

ANS.

The root bridge is usually connected to the main wired backbone LAN. Since the radio traffic from the other bridge's LANs pass through this unit, the root unit is usually connected to the LAN that originates or receives the most traffic.A non-root bridge is sometimes referred to as a remote or repeater bridge.

b) Explain the difference between SNMPv 1,2 and 3 along with its configurations.

ANS.

SNMPv1

SNMPv1 is the first version of SNMP. Although it has achieved its goal of becoming an open standard protocol, it turns out that for some applications, it lacks key areas. Many of these issues have been fixed in later versions.

SNMPv2

SNMPv2 is a sub-version of SNMPv2. Compared with the previous version, its main advantage is the Inform command. Unlike traps that are only received by managers, Informs can be positively identified through response messages. If the administrator does not respond to the Inform, the SNMP agent will resend the Inform.

Other benefits include:

• Better error handling

• Improved SET command

SNMP V3

SNMPv3 is the latest version of SNMP. Its main function is to enhance security.

The "Engine ID" identifier in SNMPv3 uniquely identifies each SNMP entity. If two SNMP entities have duplicate Engine IDs, conflicts may occur. Engine ID is used to generate a key for verified messages.

SNMPv3 security mainly has two forms:

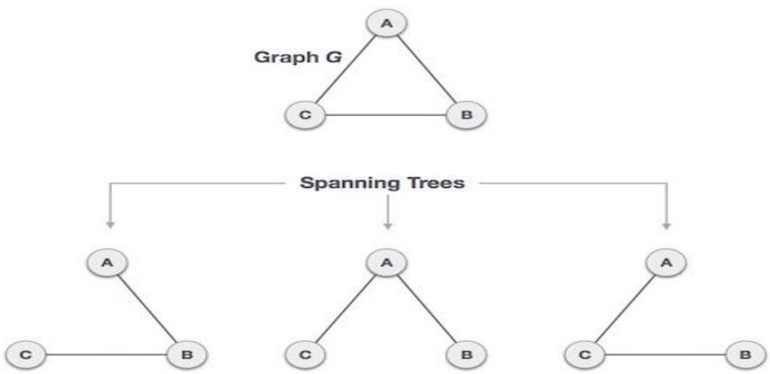
• Authentication is used to ensure that the trap is only read by the intended recipient. When creating messages, they will be provided with a special key based on the entity's Engine ID. The key is shared with the intended recipient and used to receive messages.

•Privacy encrypts the payload of SNMP messages to ensure that unauthorized users cannot read it. All traps captured will be full of garbled characters and will be unreadable. Privacy is particularly useful in applications that must route SNMP messages over the Internet.

c) Explain the spanning tree algorithm with an example.

ANS.

The spanning tree is a subset of the graph G, all vertices of the graph G cover the least number of possible edges. Therefore, the spanning tree has no cycles and therefore cannot be disconnected. Through this definition, we can draw the conclusion that every connected and undirected graph G has at least one spanning tree. The disconnected graph does not have a spanning tree because it cannot expand to all its vertices.



We found three spanning trees off one complete graph. A complete undirected graph can have maximum nn-2 number of spanning trees, where n is the number of nodes. In the above addressed example, n is 3, hence 33−2 = 3 spanning trees are possible.

We found that three trees covered the whole picture. A complete undirected graph can contain at most nn-2 spanning trees, where n is the number of nodes. In the example discussed above, n is 3, so 33-2 = 3 spanning trees are possible.

General Spanning Tree Properties

Now we know that a graph can have multiple spanning trees. Here are some attributes of the spanning tree connected to graph G −

• The connected graph G can have multiple spanning trees.

• All possible trees of graph G have the same number of edges and vertices.

• The spanning tree has no cycles (cycles).

• Deleting the edges of the spanning tree will make the graph disconnected, that is, the spanning tree has the least connections.

• Adding an edge to the spanning tree creates a circuit or a loop, that is, the spanning tree is acyclic at best.

Mathematical properties of spanning tree

• The spanning tree has n-1 edges, where n is the number of nodes (vertices).

• From a complete graph, by deleting at most e-n + 1 edges, we can build a spanning tree.

• The complete graph can contain up to nn-2 covering trees.

Therefore, we can conclude that the spanning tree is a subset of the connected G graph, while the unconnected graph has no spanning tree.

<u>Q3: a) What is the difference between a Circuit Switching and Packet Switching?</u>

ANS.

Circuit switching and packet switching are two different switching methods used to connect multiple communication devices to each other. The main difference between circuit switching and packet switching is that packet switching is connectionless, while circuit switching is connection-oriented.These are the two most common switching methods. We will see how these two processes affect the data transfer from sender to receiver are different from each other.The main difference between circuit switching and packet switching is that circuit switching is connection-oriented, while packet switching is connectionless. Let's use the comparison table below to understand more differences between circuit switching and packet switching.

<u>b) What is a DHCP protocol and why it’s important? Also explain how DHCP server works?</u>

ANS.

Dynamic Host Configuration Protocol (DHCP) is a network management protocol that is used to automatically configure devices on an IP network so that they can use network services such as DNS, NTP and any communication-based protocol via UDP or TCP. DHCP stands for Dynamic Host Configuration Protocol, which is a network protocol used on IP networks, where the DHCP server automatically assigns an IP address and other information to each host on the network so that they can communicate effectively with other hosts. Endpoint. In addition to the IP address, DHCP also assigns a subnet mask, default gateway address, domain name server (DNS) address and other related configuration parameters. Request for Comments (RFCs) 2131 and 2132 define DHCP as a standard defined by the Internet Engineering Task Force (IETF) based on the BOOTP protocol.

1. Automatic management of IP addresses, including preventing duplicate IP address problems

2. Support BOOTP client, so you can easily transition the network from BOOTP to DHCP

3. Allow the administrator to set the lease time, even on manually assigned IP addresses.

4. Allow to restrict which MAC addresses provide dynamic IP addresses

5. Allow the administrator to configure other DHCP option types outside the scope of BOOTP possible configuration

6. Allow to define one or more IP address pools that can be dynamically allocated. The user may have a server that forces the pool to be an entire subnet or network. The server should not force such pools to consist of consecutive IP addresses.

7. It is allowed to associate two or more dynamic IP address pools on a single IP network (or subnet). This is the basic support for the auxiliary network. It allows the router to act as a BOOTP relay for interfaces with multiple IP network or subnet IP addresses.

WORKS

Without entering the relevant technical information (DORA process), the DHCP client will ask for the IP address of the DHCP server for a certain period of time, during which time the DHCP client can use the dynamic IP address provided by the DHCP server. Called lease, just like the name: lease means that if the client wants to continue to use a specific IP address in which the client needs to reassign the address, the client "leases" the IP address from the DHCP server for a specific time. Renewing the lease, if the client is still on the network, will happen before the lease expiration date. In more depth, the DHCP service works by using the DORA (discover, provide, request and confirm) process (you can use a network monitoring utility to track the entire process):

c) Why we use IP Tunneling? What are the disadvantages of tunneling?

ANS.

An IP tunnel is an Internet Protocol (IP) network communications channel between two networks. It is used to transport another network protocol by encapsulation of its packets.

IP tunnels are often used for connecting two disjoint IP networks that don't have a native routing path to each other, via an underlying routable protocol across an intermediate transport network.

Disadvantages

Increase packet size

Increase processing time (and need processing power)

Elevated management of tunnel entrances and exits

of course…

1 is more attractive than 0 (invalid)

So many search plugins use tunnels

Till now, we saw the top benefits of IPSec. Unfortunately, IPSec is not free from demerits too.

From our experience in managing VPN servers, our Support Engineers often stumble upon IPSec disadvantages too. Let’s take a look at them

CPU Overhead

Having to perform encryption and decryption on the hundreds of megabytes of data flowing through the machines requires quite a bit of processing power, and this translates to **higher processor loads**.

Compatibility Issues

IPsec is a standardized solution today, and yet, some large software developers may not adhere to it, and may go ahead with standards of their own. As a result, this can lead to **compatibility issues**.

Broken Algorithms

Some of the security algorithms that are still being used in IPsec have already been cracked. This poses a huge security risk, especially if the network administrators unknowingly use those algorithms instead of newer, more complex ones that are already available

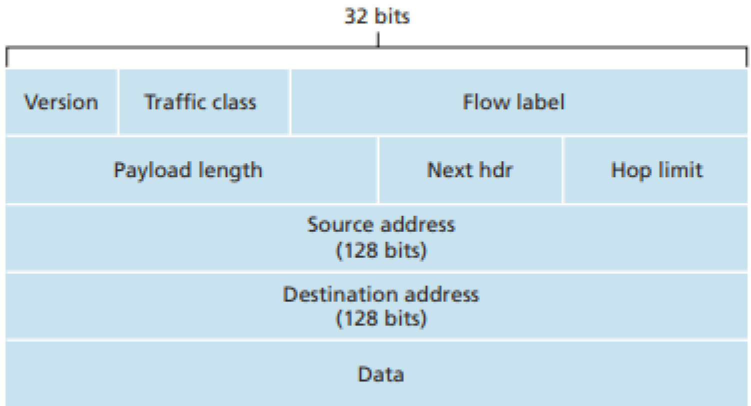
d) Explain the Internet control message protocol (ICMP) and Datagram Format.

ANS.

The Internet Control Message Protocol (ICMP) is a network layer protocol used by network devices to diagnose network communication issues. ICMP is mainly used to determine whether or not data is reaching its intended destination in a timely manner. Commonly, the ICMP protocol is used on network devices, such as routers. ICMP is crucial for error reporting and testing, but it can also be used in distributed denial-of-service (DDoS) attacks.The ICMP packet is encapsulated in an IPv4 packet. The packet consists of header and data sections. The ICMP header starts after the IPv4 header and is identified by IP protocol number '1'. All ICMP packets have an 8-byte header and variable-sized data section. The first 4 bytes of the header have fixed format, while the last 4 bytes depend on the type/code of that ICMP packet.

Datagram Format

The format of the IPv6 datagram is shown in Figure The most important changes introduced in IPv6 are evident in the datagram format: • Expanded addressing capabilities. IPv6 increases the size of the IP address from 32 to 128 bits. This ensures that the world won't run out of IP addresses. Now, every grain of sand on the planet can be IP-addressable. In addition to unicast and multicast addresses, IPv6 has introduced a new type of address, called an anycast address, which allows a datagram to be delivered to any one of a group of hosts. (This feature could be used, for example, to send an HTTP GET to the nearest of a number of mirror sites that contain a given document.) • A streamlined 40-byte header. As discussed below, a number of IPv4 fields have been dropped or made optional. The resulting 40-byte fixed-length header allows


32 bits
Version
Traffic class
Flow label
Payload length
Next hdr
Hop limit
Source address
(128 bits)
Destination address
(128 bits)
Data