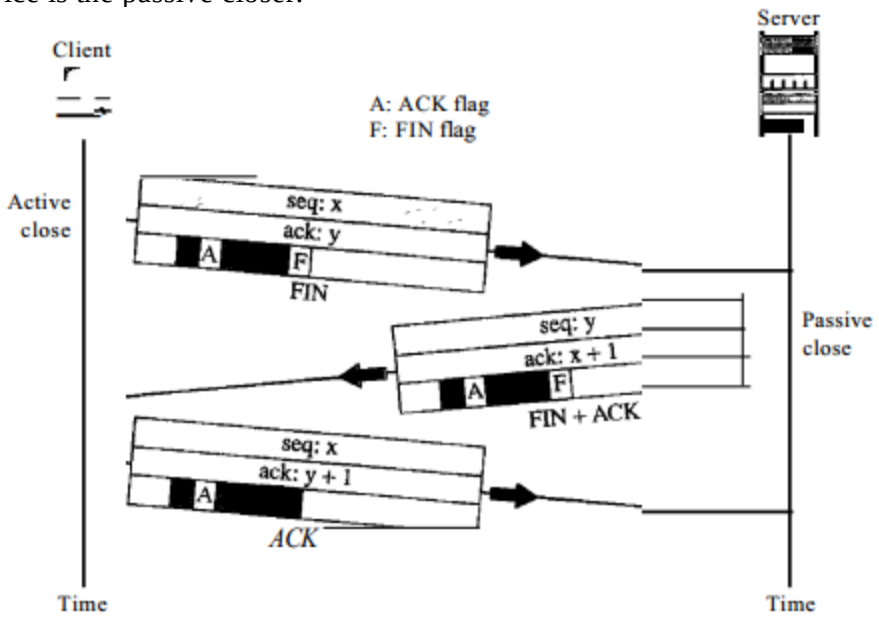
between two devices. Here's a breakdown of the three-way handshake for connection termination in TCP:
Initiating the Connection Termination: The device that wishes to terminate the connection (referred to as the active closer) sends a TCP segment with the FIN (Finish) flag set to the other device, indicating its intention to close the connection.
Acknowledgment of the Termination Request: Upon receiving the FIN segment, the receiving device (passive closer) acknowledges the termination request by sending an acknowledgment (ACK) TCP segment back to the active closer. The ACK acknowledges the receipt of the FIN segment.
Finalizing the Connection Termination: After sending the ACK, the passive closer also sends its own FIN segment to the active closer, indicating its agreement to close the connection. This segment has the FIN flag set.
Acknowledgment of the Final Termination: Upon receiving the FIN segment from the passive closer, the active closer acknowledges it by sending an ACK segment back. This ACK serves as confirmation that the passive closer's FIN has been received.
At this point, both devices have exchanged FIN and ACK segments, indicating their mutual agreement to terminate the connection. The connection is considered closed after this three-way handshake for connection termination has taken place.
It's worth noting that either device can initiate the connection termination by sending the first FIN segment. The device that sends the first FIN segment is known as the active closer, while the other device is the passive closer.



Connection termination using three-way handshaking

User Datagram Protocol(UDP)

The User Datagram Protocol (UDP) is called a connectionless, unreliable transport protocol. It does not add anything to the services of IP except to provide process-to process communication instead of host-to-host communication. Also, it performs very limited error checking.

SAQ's-Self Assessment Questions

Which of the following is false with respect to TCP?
a) Connection-oriented
b) Process-to-process
c) Transport layer protocol

d) Unreliable
Answer: d
In TCP, sending and receiving data is done as _____
a) Stream of bytes
b) Sequence of characters
c) Lines of data
d) Packets
Answer: a
TCP process may not write and read data at the same speed. So we need _____ for storage.
a) Packets
b) Buffers
c) Segments
d) Stacks
Answer: b
TCP groups a number of bytes together into a packet called _____
a) Packet
b) Buffer
c) Segment
d) Stack
Answer: c
Communication offered by TCP is _____
a) Full-duplex
b) Half-duplex
c) Semi-duplex
d) Byte by byte
Answer: a
To achieve reliable transport in TCP, _____ is used to check the safe and sound arrival of data.
a) Packet
b) Buffer
c) Segment
d) Acknowledgment
Answer: d
In segment header, sequence number and acknowledgement number fields refer to _____
a) Byte number
b) Buffer number
c) Segment number
d) Acknowledgment
Answer: a
Suppose a TCP connection is transferring a file of 1000 bytes. The first byte is numbered 10001. What is the sequence number of the segment if all data is sent in only one segment?
a) 10000
b) 10001
c) 12001
d) 11001
Answer: b
Bytes of data being transferred in each connection are numbered by TCP. These numbers start with a _____
a) Fixed number
b) Random sequence of 0's and 1's
c) One
d) Sequence of zero's and one's

Answer: d
The value of acknowledgement field in a segment defines _____
a) sequence number of the byte received previously
b) total number of bytes to receive
c) sequence number of the next byte to be received
d) sequence of zeros and ones
Answer: c
With reference to UDP, which of the following statements are true?
A. Before transmission, UDP serializes the packets
B. Error checking is done by UDP before transmission
C. UDP is a high latency protocol
D. UDP is a connectionless protocol
Answer: D
One of the responsibilities of the transport layer protocol is to create a ___ communication.
A. host-to-host
B. Process-to-process
C. node-to-node
D. None of the above
Answer: B
TCP is a _____ protocol.
A.stream-oriented
B. Message-oriented
C. Block-oriented
D. None of the above
Answer: A
TCP groups a number of bytes together into a packet called a _____
A. user datagram
B. Segment
C. datagram
D. none of the above
Answer: B
TCP is a _____ protocol
A. unreliable
B. best-effort delivery
C. reliable
D. none of the above
Answer: C
16. How does TCP handle congestion control?
a) By dropping packets indiscriminately
b) By retransmitting all lost packets immediately
c) By slowing down the rate of packet transmission
d) By increasing the size of the send window
17. Which TCP flag is used to initiate a connection between two devices?
a) SYN
b) ACK
c) RST
d) FIN
18. How does TCP ensure reliable data delivery?
a) By using flow control mechanisms
b) By implementing error detection and retransmission
c) By assigning unique sequence numbers to each packet
d) By applying checksums to verify packet integrity
19. What is the maximum number of TCP ports available?
a) 65,536

b) 256
c) 1024
d) 4,294,967,296
20. Which TCP feature allows multiple packets to be combined into a single larger packet for efficiency?
a) Windowing
b) Fragmentation
c) Segmentation
d) Congestion control

11. Summary
TCP is a reliable, connection-oriented protocol suitable for applications that require guaranteed delivery of data, UDP is a lightweight, connectionless protocol suitable for real-time applications with low latency requirements, and FCP is a protocol used in storage networks for high-speed and reliable data transfer between servers and storage devices.
12. Terminal Questions
What is the purpose of the TCP three-way handshake?
Explain the difference between TCP and UDP.
What is the TCP sliding window mechanism, and how does it improve performance?
Describe the purpose and function of the TCP sequence number and acknowledgment number fields.
How does TCP handle congestion control? Explain the congestion control algorithms used in TCP.
What is the significance of the SYN and ACK flags in TCP?
How does TCP ensure reliable data delivery?

Topic 3: Domain Name System

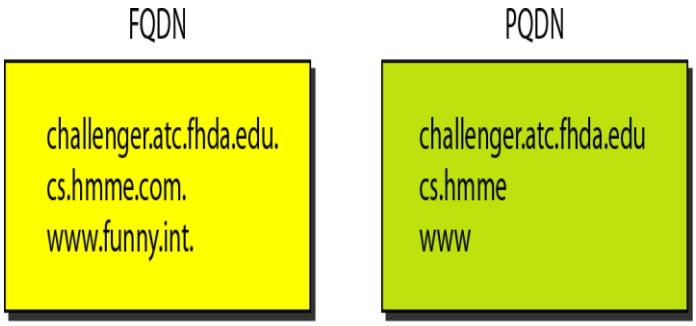
Domain Name System
There are several applications in the application layer of the Internet model that follow the client/server paradigm. The client/server programs can be divided into two categories: those that can be directly used by the user, such as e-mail, and those that support other application programs. The Domain Name System (DNS) is a supporting program that is used by other programs such as e-mail.
NAME SPACE
To be unambiguous, the names assigned to machines must be carefully selected from a name space with complete control over the binding between the names and IP addresses. In other words, the names must be unique because the addresses are unique. A name space that maps each address to a unique name can be organized in two ways: fiat or hierarchical.

Fully Qualified Domain Name
If a label is terminated by a null string, it is called a fully qualified domain name (FQDN). An FQDNis a domain name that contains the full name of a host. It contains all labels, from the most specific tothe most general, that uniquely define the name of the host. For example, the domain name challenger.ate.tbda.edu. is the FQDN of a computer named challenger installed at the

Advanced Technology Center (ATC) at De Anza College. A DNS server can only match an FQDN to an address. Note that the name must end with a null label, but because null means nothing, the label ends with a dot (.).

Partially Qualified Domain Name

If a label is not terminated by a null string, it is called a partially qualified domain name (PQDN). A PQDN starts from a node, but it does not reach the root. It is used when the name to be resolved belongs to the same site as the client. Here the resolver can supply the missing part, called the suffix, to createan FQDN. For example, if a user at the jhda.edu. site wants to get the IP address of the challenger computer, he or she can define the partial name challenger The DNS client adds the suffix atc.jhda.edu. before passing the address to the DNS server



Zones and domains

Zones are typically defined by creating a zone file, which contains the DNS records for the domain and its subdomains.

A domain refers to a hierarchical naming structure used to identify resources on the internet. It is a human-readable name that represents an organization, website, or network. For example, "example.com" is a domain name. s the authoritative DNS server for that particular zone.

Topic4: Fiber Channel Protocol; Stream Control Transmission Protocol

Fibre Channel is a high-speed networking technology primarily used for transmitting data among data centers, computer servers, switches, and storage at data rates of up to 128 Gbps with distances up to 10Km.

Fibre Channel Protocol (FCP) is the SCSI (Small Computer System Interface) interface protocol operating on an established Fibre Channel connection. As Fibre Channel provides us with a high-speed data transfer service it can be used to connect workstations, mainframes, displays, storage devices, and supercomputers. The FCP provides one standardized way for storage, data transfer, and networking as the main task of the FCP is to ensure the successful transfer of large and bulky information/ data so that the manufacturers can easily support a variety of channels and networks. The Fibre Channel protocol, also known as FC, is a method for transferring data serially over copper or optical fiber in order to achieve lower latency and faster speeds. It is a SCSI interface protocol that utilizes Fibre Channel connections. This protocol is used to connect high-performance

computers, storage devices, mainframes, big data workstations, and displays as virtual big data structured screens.
So, Fibre Channel is primarily used to connect computer data storage to servers in storage area networks (SAN) in commercial data centers. Though fiber channel mainly runs on optical fiber cables it is also capable of transmitting over copper cables. As mentioned earlier, fiber channels can transmit data up to 128 Gbps (Gigabits per second) hence the alternate name Gigabit Fibre Channel (GFC).

FC Layers

When it comes to learning the various layers of Fibre Channel it is important to understand that FC does not follow the traditional OSI 7 layer model. Instead, it is broken down into 5 layers. As shown below:

FC-0 - Defines the physical media used to link two Fibre Channel ports, including cabling types, optical and electrical parameters for a variety of data rates, maximum transfer distances, and noise limits. Fibre Channel supports two types of cables: Copper and optical.[2]

FC-1 - Defines the transmission protocol including serial encoding and decoding rules, special characters and error control.[3]

FC-2 - Defines the transport mechanism of Fibre Channel and the framing rules of the data to be transferred between ports, the different mechanisms for controlling the service of classes and the means of managing the sequence of a data transfer.[4]

FC-3 - Defines common services required for advanced features such as striping, hunt group, and multicast.

FC-4 - Defines the application interfaces that can execute over Fibre Channel. It specifies the mapping rules of upper layer protocols using the FC levels below.[5]

FCP Topologies:

DAS (Direct Attached Storage)

NAS (Network Attached Storage)

SAN (Storage Area Network)

1.3 FCP Ports:

N Port (The Node Port)

F Port (The Fabric Port)

L Port (The Loop Port)

FL Port (The Fabric Loop Port)

E Port (The Extension Port)

G Port (The Generic Port)

GL Port (The Generic Loop Port)

SL Port (The Segmented Loop Port)

TL Port (The Translated Loop Port)

T Port (The Trunk Port)

There are two main protocols for fiber channels with regard to block storage:

Fibre channel protocol (FCP): covered in the article

FICon (Fibre Connection) is a protocol that transports ESCon (Enterprise Systems Connection) commands, used by IBM mainframe computers, over Fibre Channel.

1.4 FCP Features Fibre Channel:

Data transfer speed of up to 128Gbps over a distance of 10Km.

Both Fiber optic cable and copper cables can be used.

FCP is used to transmit SCSI (Small Computer System Interface) commands over a Fibre Channel Network (FCN)

The Fibre Channel Protocol (FCP) is an original protocol used in Storage Area Network (SAN).

SFP (Small Form-factor Pluggable) connectors are used to facilitate a reliable, wired, high-speed connection.

The Fibre Channel Protocol (FCP) offers a bandwidth range of 100 MB/s to 1.6 GB/s and

can support distances of up to 500 meters to 10 kilometers.
FCP operates similarly to both TCP and UDP protocols.
The Fibre Channel Protocol (FCP) is both reliable and stable, with a balanced design.
In Fibre Channel Protocol (FCP), World Wide Names (WWN) are used for addressing.
These 8-byte addresses consist of 16 hexadecimal characters.
The Fibre Channel Protocol (FCP) uses a format such as 15:00:00:f0:8c:95:de.
Ability to carry multiple existing interface command sets, including Internet Protocol (IP), SCSI, IPI, HIPPI-FP, and audio/video.
Support for multiple cost/performance levels, from small systems to supercomputers.
In Fibre Channel Protocol (FCP), a dedicated host bus adapter, specialized cables, and switches are used. It is distinct from Ethernet at all layers of the OSI model, including the physical layer

1.5 World Wide Name (WWN):

A **World Wide Name (WWN) or World Wide Identifier (WWID)** is a unique identifier used in storage technologies like Fibre Channel. It is a unique identifier that is hard-coded into each Fibre similar to how devices have MAC Addresses. It is a 64-bit or 128-bit name and is assigned by the **Institute of Electrical and Electronics Engineers IEEE**. Each network storage device that a manufacturer produces must include the manufacturer's WWN, in order to help system administrators (SA) uniquely categorize and identify storage segments.
The WWN looks for example:
15:00:00:f0:8c:08:95:de

Types of World Wide Name (WWN):

There are majorly two types of WWNs implemented in an FC Storage Area Network (SAN):
World Wide Node Name (WWNN): A World Wide Node Name, WWNN, or WWnN, is a World Wide Name assigned to a node (an endpoint, a device) in a Fibre Channel fabric.
World Wide Port Name (WWPN): a World Wide Port Name, WWPN, or WWpN, is a World Wide Name assigned to a port in a Fibre Channel fabric. In order to behave as a unique identifier in the network, it works similarly to the MAC address in Ethernet protocol.
Fibre Channel Protocol (FCP) uses World Wide Node Names (WWNN) to identify nodes in data storage networks. These names can identify multiple network interfaces on a single node. The WWPN (World Wide Port Name) can also be derived from the WWNN.
In Fibre Channel Protocol (FCP), a unique World Wide Port Name (WWPN) is assigned to every individual port on a node.
In Fibre Channel Protocol (FCP), a multiport Host Bus Adapter (HBA) will have a different number of World Wide Port Names (WWPNs) for each port. WWPNs are similar to the MAC address in Ethernet networks.
In Fibre Channel Protocol (FCP), World Wide Port Names (WWPN) are burn-in by the manufacturer. They are validated to be globally unique.
In Fibre Channel Protocol (FCP), World Wide Port Names (WWPNs) are assigned to Host Bus Adapters (HBAs) on both client and storage systems.
In Fibre Channel Protocol (FCP), World Wide Port Names (WWPNs) are given more importance when configuring Fibre Channel Networks, compared to World Wide Node Names (WWNNs).
In Fibre Channel Protocol (FCP), World Wide Port Names (WWPNs) cannot be changed once assigned.

1.6 Advantages of Fibre Channel:

FCP has high performance
provides good backup and restoration and simplified consolidation
also offers congestion-free data flow, Gigabit bandwidth, compatibility with multiple topologies and protocols, flow control, and self-management
It is providing high-speed data transfer

It is cost-efficient
High-speed data can be transferred over a distance of 10km
supports several fault-tolerant features
FCP having good bandwidth and speed
The FCP protocol utilizes data frames for transmitting information over a network, which can be used for both link-level and device-level communications
FCP having good Flow Control
The Fibre Channel protocol (FCP) is known for its balanced and reliable nature, providing stable communication between devices
FCP is a balanced and reliable protocol that is used to transmit SCSI (Small Computer System Interface) commands over Fibre Channel Networks (FCN)

1.7 Disadvantage of Fibre Channel:

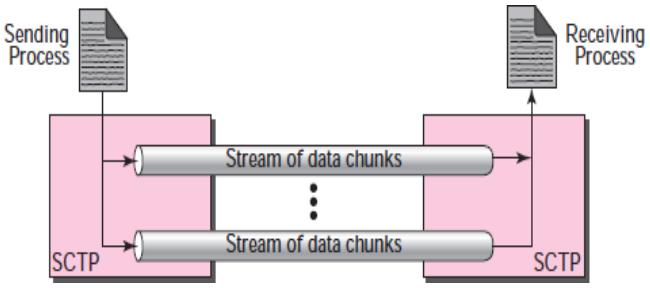
FCP can be more expensive in cost compared to iSCSI
FCP can be more costly and complex to implement
FCP requires updating the cards within servers
also purchasing FC cables and switches
More expensive than SCSI (Small Computer System Interface)
More complex than SCSI (Small Computer System Interface)
More equipment/ overhead (like FC cables, switches, etc.,) is required
Ports/Links
Port Types
There are a number of FC port types. Below outlines the main ones:

	Port Type	Port Name	Port Description
	G_Port	Generic	This is the port type that all ports first start with, prior to transitioning to another port type.
	F_Port	Fabric	Connects to an N_Port (aka Initiator or Target)
	N_Port	Node	The Initiator or Target. Connects to an F_Port (aka Fabric switch).
	E_Port	Extension	Connects to another fabric switch.

Stream Control Transmission Protocol (SCTP)
SCTP is designed as a general-purpose transport layer protocol that can **handle multimedia andstream traffic**, which are increasing every day on the Internet.
Note: SCTP is a ***message-oriented, reliable protocol*** that combines the best features of UDP and TCP.
We briefly compare UDP, TCP, and SCTP:
UDP is **a message-oriented protocol**. A process delivers a message to UDP, which is
encapsulated in a user datagram and sent over the network. UDP *conserves the message boundaries;* each message is independent from any other message. UDP is unreliable; the sender cannot know the destiny of messages sent. A message can be lost, duplicated, or received out of order. UDP also lacks some other features, such as congestion control and flow control, neededfor a friendly transport-layer protocol.
TCP is **a byte-oriented protocol**. It receives a message or messages from a process, stores them
as a stream of bytes, and sends them in segments. There is no preservation of the message boundaries. However, TCP is a reliable protocol. The duplicate segments are detected, the lost segments are resent, and the bytes are delivered to the end process in order. TCP also has

congestion control and flow control mechanisms.
SCTP combines the best features of UDP and TCP. SCTP is a **reliable message-oriented**
protocol. It preserves the message boundaries and at the same time detects lost data, duplicate data, and out-of-order data. It also has congestion control and flow control mechanisms.

SCTP SERVICES



Process-to-Process Communication: SCTP uses all well-known ports in the TCP space.

Multiple Streams
SCTP allows **multistream service** in each connection, which is called **association** in SCTP terminology. If one of the streams is blocked, the other streams can still deliver their data.
FIG 1.1 Multiple Streams
1.2.2 Multihoming
- **Multihomed:** host connected to more than one physical address with multiple IP addresses, only oneof these IP addresses per end can be utilized during the connection.
Note: *SCTP association allows multiple IP addresses for each end.*

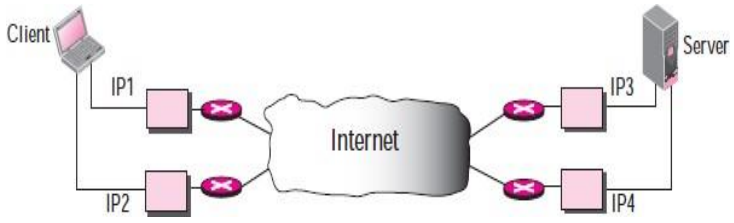


FIG **Multihomed**

Full-Duplex Communication
SCTP offers **full-duplex service.** Each SCTP then has a sending and receiving buffer and packets are sent in both directions.

Connection-Oriented Service
SCTP is a connection-oriented protocol. However, in SCTP, a connection is called an **association.** When a process at site A wants to send and receive data from another process at site B, the following occurs:
The two SCTPs establish an association between each other.
Data are exchanged in both directions.
The association is terminated.

Reliable Service
SCTP is a reliable transport protocol. It uses an acknowledgment mechanism to check the safe andsound arrival of data.

SCTP FEATURES

Transmission Sequence Number (TSN)
The unit of data in SCTP is a data chunk. Data transfer in SCTP is controlled by numbering the data chunks. SCTP uses a **transmission sequence number (TSN)** to number the data chunks. In other words, the TSN in SCTP plays the analogous role as the sequence number in TCP. TSNs are 32 bits long and randomly initialized between **0** and $\mathbf{2^{32} - 1}$. Each data chunk must carry the corresponding TSN in its header.
Stream Identifier (SI)
In SCTP, there may be several streams in each association. Each stream in SCTP needs to be identifiedusing a **stream identifier (SI).** Each data chunk must carry the SI in its header so that when it arrives at the destination, it can be properly placed in its stream. The SI is a 16-bit number starting from 0.

Stream Sequence Number (SSN)
To distinguish between different data chunks belonging to the same stream, SCTP uses SSNs. When a data chunk arrives at the destination SCTP, it is delivered to the appropriate stream and inthe proper order. This means that, in addition to an SI, SCTP defines each data chunk in each stream with a stream sequence number (SSN).

SAQ's-Self Assessment Questions

1. Which layer of the OSI model does Fibre Channel Protocol operate on?
   a) Network layer
   b) Transport layer
   c) Data link layer
   d) Application layer
   Answer: c) Data link layer

2. What is the primary purpose of Fibre Channel Protocol?
   a) File sharing
   b) Data encryption
   c) Storage area networking
   d) Internet routing
   Answer: c) Storage area networking

3. Fibre Channel Protocol is primarily used for connecting:
   a) Servers to servers
   b) Servers to storage devices
   c) Routers to switches
   d) Workstations to printers
   Answer: b) Servers to storage devices

4. Which physical medium is commonly used for Fibre Channel connections?
   a) Twisted-pair copper cables
   b) Coaxial cables
   c) Fiber-optic cables
   d) Wireless connections
   Answer: c) Fiber-optic cables

5. What is the maximum data rate supported by Fibre Channel Protocol?
a) 100 Mbps
b) 1 Gbps
c) 10 Gbps
d) 100 Gbps
Answer: d) 100 Gbps

6. Which topology is commonly used in Fibre Channel networks?
a) Bus
b) Ring
c) Star
d) Mesh
Answer: c) Star

7. Fibre Channel Protocol uses _____ addressing scheme.
a) MAC
b) IP
c) FC-ID
d) VLAN
Answer: c) FC-ID

8. Which layer of Fibre Channel Protocol is responsible for flow control?
a) FC-0
b) FC-1
c) FC-2
d) FC-3
Answer: b) FC-1

9. What is the purpose of zoning in Fibre Channel networks?
a) Data encryption
b) Load balancing
c) Access control
d) Error correction
Answer: c) Access control

10. Which Fibre Channel Protocol layer provides reliable delivery of frames?
a) FC-0
b) FC-1
c) FC-2
d) FC-3
Answer: c) FC-2

11. What does SCTP stand for?
a) Secure Control Transmission Protocol
b) Simple Control Transfer Protocol
c) Stream Control Transmission Protocol
d) Secure Channel Transmission Protocol
Answer: c) Stream Control Transmission Protocol

12. SCTP is a transport layer protocol that operates:
a) In connectionless mode
b) In connection-oriented mode
c) In multicast mode
d) In broadcast mode
Answer: b) In connection-oriented mode

13. Which layer of the OSI model does SCTP operate on?
a) Network layer
b) Transport layer
c) Data link layer
d) Application layer
Answer: b) Transport layer

14. Which of the following is NOT a feature of SCTP?
a) Multihoming
b) Ordered delivery of messages
c) Congestion control
d) Connectionless communication
Answer: d) Connectionless communication

15. How many streams are available in SCTP?
a) 1
b) 2
c) 4
d) Unlimited
Answer: d) Unlimited

16. What is the primary advantage of multihoming in SCTP?
a) Load balancing
b) Improved reliability
c) Faster transmission speed
d) Simultaneous connections over multiple network interfaces
Answer: d) Simultaneous connections over multiple network interfaces

17. Which of the following is a valid SCTP port number?
a) 53
b) 80
c) 443
d) 36412
Answer: d) 36412

18. SCTP uses _____ for message fragmentation and reassembly.
a) Segments
b) Packets
c) Fragments
d) Frames
Answer: c) Fragments

19. SCTP provides _____ service to its users.
a) Reliable, connectionless
b) Reliable, connection-oriented
c) Unreliable, connectionless
d) Unreliable, connection-oriented
Answer: b) Reliable, connection-oriented

20. Which of the following is NOT a valid SCTP primitive?
a) SCTP-SEND
b) SCTP-RECEIVE
c) SCTP-OPEN

d) SCTP-CLOSE
Answer: b) SCTP-RECEIVE

Topic 5: Congestion Control: Open Loop, Closed Loop Choke Packets

DATA TRAFFIC
The main focus of congestion control and quality of service is data traffic. In congestion control we try to avoid traffic congestion. In quality of service, we try to create an appropriate environment for the traffic. So, before talking about congestion control and quality of service, we discuss the data traffic itself.

Traffic Descriptor

Traffic descriptors are qualitative values that represent a data flow. Figure shows a traffic flow with some of these values.

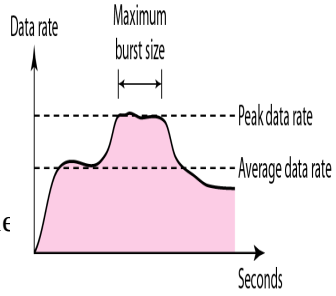


Fig: Traffic de

Average Data Rate

The average data rate is the number of bits sent during a period of time, divided by the number of seconds in that period. We use the following equation:

Average data rate = amount of data / time

The average data rate is a very useful characteristic of traffic because it indicates the average bandwidth needed by the traffic.

Peak Data Rate

The peak data rate defines the maximum data rate of the traffic. In the above Figure, it is the maximum *y* axis value. The peak data rate is a very important measurement because it indicates the peak bandwidth that the network needs for traffic to pass through without changing its data flow.

Maximum Burst Size

Although the peak data rate is a critical value for the network, it can usually be ignored if the duration of the peak value is very short. For example, if data are flowing steadily at the rate of 1 Mbps with a sudden peak data rate of 2 Mbps for just 1 ms, the network probably can handle the situation. However, if the peak data rate lasts 60 ms, there may be a problem for the network. The maximum burst size normally refers to the maximum length of time the traffic is generated at the peak rate.

Effective Bandwidth

The effective bandwidth is the bandwidth that the network needs to allocate for the flow of traffic. The effective bandwidth is a function of three values: average data rate, peak data rate, and maximum burst size. The calculation of this value is very complex.

3.5.1.2 Traffic Profiles

For our purposes, a data flow can have one of the following traffic profiles: constant bit rate, variable bit rate, or bursty as shown in Figure.

Constant Bit Rate

A constant-bit-rate (CBR), or a fixed-rate, traffic model has a data rate that does not change. In this type of flow, the average data rate and the peak data rate are the same.
The maximum burst size is not applicable. This type of traffic is very easy for a network to handle since it is predictable. The network knows in advance how much bandwidth to allocate for this type of flow.

Variable Bit Rate

In the variable-bit-rate (VBR) category, the rate of the data flow changes in time, with the changes smooth instead of sudden and sharp. In this type of flow, the average data rate and the peak data rate are different. The maximum burst size is usually a small value. This type of traffic is more difficult to handle than constant-bit-rate traffic, but it normally does not need to be reshaped, as we will see later.

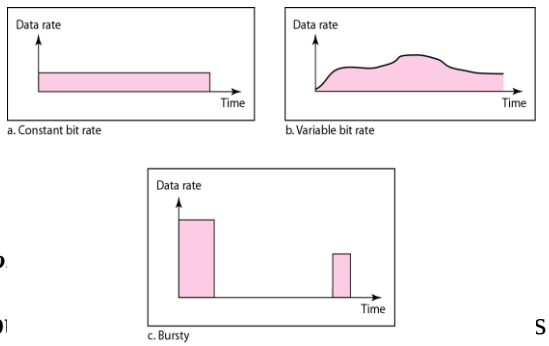


Fig a) ***Co***

Bursty

In the **b** s suddenly in a very short time. It may jump from zero, for example, to 1 Mbps in a few microseconds and vice versa. It may also remain at this value for a while. The average bit rate and the peak bit rate are very different values in this type of flow. The maximum burst size is significant. This is the most difficult type of traffic for a network to handle because the profile is very unpredictable. To handle this type of traffic, the network normally needs to reshape it, using reshaping techniques, as we will see shortly. Bursty traffic is one of the main causes of congestion in a network.

CONGESTION

An important issue in a packet-switched network is **congestion.** Congestion in a network may occur if the **load** on the network-the number of packets sent to the network-is greater than the *capacity* of the network-the number of packets a network can handle.
Congestion control refers to the mechanisms and techniques to control the congestion and keep the load below the capacity. We may ask why there is congestion on a network. Congestion happens in any system that involves waiting. For example, congestion happens on a freeway because any abnormality in the flow, such as an accident during rush hour, creates blockage.

Congestion in a network or internetwork occurs because routers and switches have queues-buffers that hold the packets before and after processing. A router, for example, has an input queue and an output queue for each interface.

The packet is put at the end of the input queue while waiting to be checked.
The processing module of the router removes the packet from the input queue once it reaches the front of the queue and uses its routing table and the destination address to find the route.
The packet is put in the appropriate output queue and waits its tum to be sent.
We need to be aware of two issues. First, if the rate of packet arrival is higher than the packet processing rate, the input queues become longer and longer. Second, if the packet departure rate is less than the packet processing rate, the output queues become longer and longer.

Network Performance

Congestion control involves two factors that measure the performance of a network: *delay* and *throughput.* Figure shows these two performance measures as function of load.

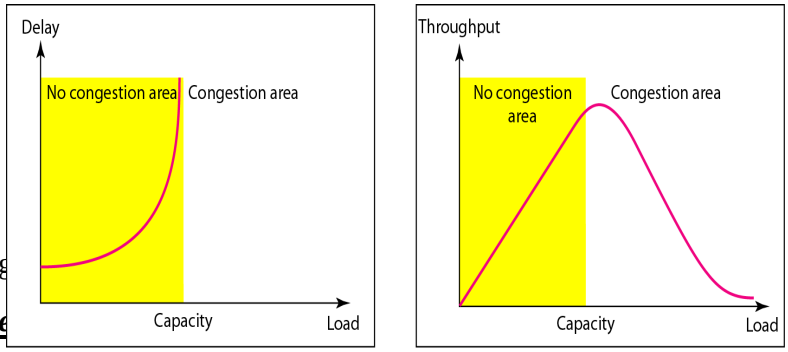


Fig a. Delay as a function of load b. Throughput as a function of load

De Ne…twork, the delay is at a minimum. This minimum delay is composed of propagation delay and processing delay, both of which are negligible. However, when the load reaches the network capacity, the delay increases sharply because we now need to add the waiting time in the queues (for all routers in the path) to the total delay. Note that the delay becomes infinite when the load is greater than the capacity. If this is not obvious, consider the size of the queues when almost no packet reaches the destination, or reaches the destination with infinite delay; the queues become longer and longer. Delay has a negative effect on the load and consequently the congestion. When a packet is delayed, the source, not receiving the acknowledgment, retransmits the packet, which makes the delay, and the congestion, worse.

Throughput Versus Load

We defined throughput in Chapter 3 as the number of bits passing through a point in a second. We can extend that definition from bits to packets and from a point to a network. We can define throughput in a network as the number of packets passing through the network in a unit of time. Notice that when the load is below the capacity of the network, the throughput increases proportionally with the *load.* We expect the throughput to remain constant after the load reaches the capacity, but instead the throughput declines sharply. The reason is the discarding of packets by the routers. When the load exceeds the capacity, the queues become full and the routers have to discard some packets. Discarding packet;'does not reduce the number of packets in the network because the sources retransmit the packets, using time-out mechanisms, when the packets do not reach the destinations.

CONGESTION CONTROL

Congestion control refers to techniques and mechanisms that can either prevent congestion, before it happens, or remove congestion, after it has happened. In general, we can divide congestion control mechanisms into two broad categories: open-loop congestion control (prevention) and closed-loop congestion control (removal) as shown in Figure

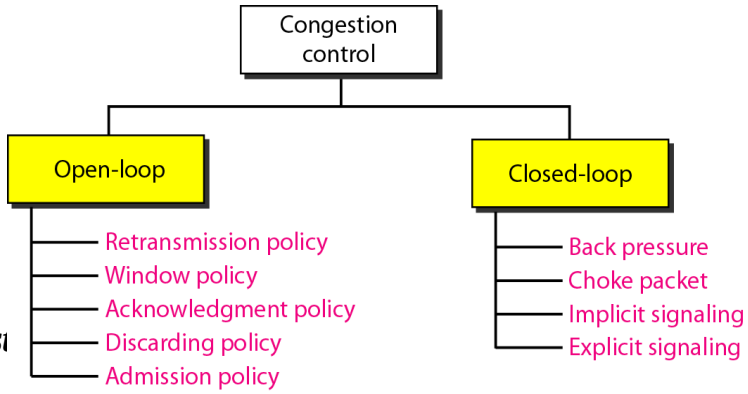


Fig. Congest

Open-Loop Congestion Control

In open-loop congestion control, policies are applied to prevent congestion before it happens. In these mechanisms, congestion control is handled by either the source or the destination. We give a brief list of policies that can prevent congestion.

Retransmission Policy

Retransmission is sometimes unavoidable. If the sender feels that a sent packet is lost or corrupted, the packet needs to be retransmitted. Retransmission in general may increase congestion in the network. However, a good retransmission policy can prevent congestion. The retransmission policy and the retransmission timers must be designed to optimize efficiency and at the same time prevent congestion.
For example, the retransmission policy used by TCP (explained later) is designed to prevent or alleviate congestion.

Window Policy

The type of window at the sender may also affect congestion. The Selective Repeat window is better than the Go-Back-N window for congestion control. In the *Go-Back-N* window, when the timer for a packet times out, several packets may be resent, although some may have arrived safe and sound at the receiver. This duplication may make the congestion worse. The Selective Repeat window, on the other hand, tries to send the specific packets that have been lost or corrupted.

Acknowledgment Policy

The acknowledgment policy imposed by the receiver may also affect congestion. If the receiver does not acknowledge every packet it receives, it may slow down the sender and help prevent congestion. Several approaches are used in this case. A receiver may send an acknowledgment only if it has a packet to be sent or a special timer expires. A receiver may decide to acknowledge only *N* packets at a time. We need to know that the acknowledgments are also part of the load in a network. Sending fewer acknowledgments means imposing less load on the network.

Discarding Policy

A good discarding policy by the routers may prevent congestion and at the same time may not harm the integrity of the transmission. For example, in audio transmission, if the policy is to discard less sensitive packets when congestion is likely to happen, the quality of sound is still

preserved and congestion is prevented or alleviated.

Admission Policy

An admission policy, which is a quality-of-service mechanism, can also prevent congestion in virtual-circuit networks. Switches in a flow first check the resource requirement of a flow before admitting it to the network. A router can deny establishing a virtual circuit connection if there is congestion in the network or if there is a possibility of future congestion.

Closed-Loop Congestion Control

Closed-loop congestion control mechanisms try to alleviate congestion after it happens. Several mechanisms have been used by different protocols. We describe a few of them here.

Backpressure

The technique of *backpressure* refers to a congestion control mechanism in which a congested node stops receiving data from the immediate upstream node or nodes. This may cause the upstream node or nodes to become congested, and they, in turn, reject data from their upstream nodes or nodes. And so on. Backpressure is a node-to-node congestion control that starts with a node and propagates, in the opposite direction of data flow, to the source. The backpressure technique can be applied only to virtual circuit networks, in which each node knows the upstream node from which a flow of data is corning. Below Figure shows the idea of backpressure.

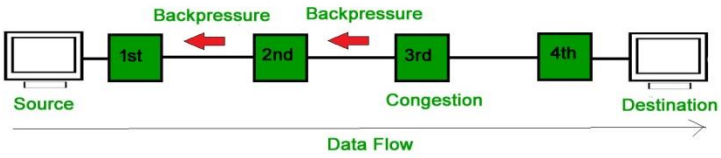
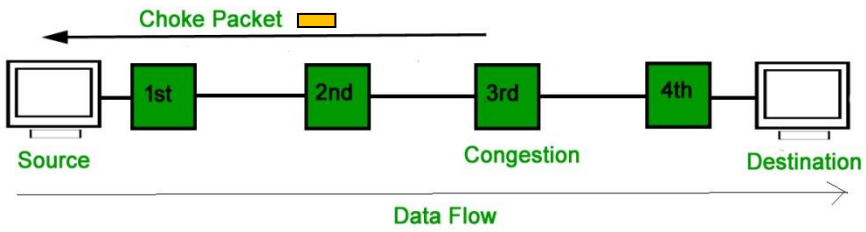


Fig. 3.5.6 Backpressure method for alleviating congestion

Node 3 in the figure has more input data than it can handle. It drops some packets in its input buffer and informs node 2 to slow down. Node 2, in turn, may be congested because it is slowing down the output flow of data. If node 2 is congested, it informs node I to slow down, which i urce of data to slow down. This, in n node 3 is moved backward to the s None o backpressure. It was, however, implemented in the first virtual-circuit network, X.25. The technique cannot be implemented in a datagram network because in this type of network, a node (router) does not have the slightest knowledge of the upstream router.

Choke Packet

A choke packet is a packet sent by a node to the source to inform it of congestion. Note the difference between the backpressure and choke packet methods. In backpressure, the warning is from one node to its upstream node, although the warning may eventually reach the source station. In the choke packet method, the warning is from the router, which has encountered congestion, to the source station directly. The intermediate nodes through which the packet has travelled are not warned. We have seen
an example of this type of control in ICMP. When a router in the Internet is overwhelmed with IP datagrams, it may discard some of them; but it informs the source host, using a source quench ICMP message. The warning message goes directly to the source station; the intermediate routers, and does not take any action. Figure shows the idea of a choke packet.



Implicit Signaling

In implicit signaling, there is no communication between the congested node or nodes and the source. The source guesses that there is a congestion somewhere in the network from other symptoms. For example, when a source sends several packets and there is no acknowledgment for a while, one assumption is that the network is congested. The delay in receiving an acknowledgment is interpreted as congestion in the network; the source should slow down. We will see this type of signaling when we discuss TCP congestion control later in the chapter.

Explicit Signaling

The node that experiences congestion can explicitly send a signal to the source or destination. The explicit signaling method, however, is different from the choke packet method. In the choke packet method, a separate packet is used for this purpose; in the explicit signaling method, the signal is included in the packets that carry data. Explicit signaling, as we will see in Frame Relay congestion control, can occur in either the forward or the backward direction.

Backward Signaling A bit can be set in a packet moving in the direction opposite to the congestion. This bit can warn the source that there is congestion and that it needs to slow down to avoid the discarding of packets.

Forward Signaling A bit can be set in a packet moving in the direction of the congestion. This bit can warn the destination that there is congestion. The receiver in this case can use policies, such as slowing down the acknowledgments, to alleviate the congestion.

SAQ's Self-Assessment Questions

What is the primary purpose of congestion control?
a) Minimizing latency
b) Maximizing throughput
c) Ensuring fair resource allocation
d) Eliminating packet loss

Which technique allows routers to influence traffic sources directly without explicit feedback from the network?
a) Open loop choke packets
b) Closed loop choke packets
c) Dynamic routing
d) Quality of Service (QoS)

How do open loop choke packets indicate congestion to traffic sources?
a) Through explicit feedback
b) By marking packets with Differentiated Services Code Points (DSCPs)
c) By reducing the transmission rate
d) By increasing the packet size

Which technique provides more precise congestion feedback to traffic sources?
a) Open loop choke packets
b) Closed loop choke packets
c) Dynamic routing
d) Quality of Service (QoS)

Which mechanism is commonly used in closed loop choke packets to indicate congestion levels?
a) Differentiated Services Code Points (DSCPs)
b) Explicit Congestion Notification (ECN)
c) TCP window size
d) Hop count
Which technique requires bidirectional communication between routers and traffic sources?
a) Open loop choke packets
b) Closed loop choke packets
c) Dynamic routing
d) Quality of Service (QoS)
Which congestion control mechanism is based on packet marking and differentiation?
a) Open loop choke packets
b) Closed loop choke packets
c) Dynamic routing
d) Quality of Service (QoS)
What is a potential disadvantage of open loop choke packets?
a) Limited control over congestion
b) High communication overhead
c) Inefficient resource utilization
d) Increased latency
Which congestion control technique is commonly used in real-time multimedia streaming?
a) Open loop choke packets
b) Closed loop choke packets
c) Dynamic routing
d) Quality of Service (QoS)
Which technique offers simplicity and efficiency in congestion control?
a) Open loop choke packets
b) Closed loop choke packets
c) Dynamic routing
d) Quality of Service (QoS)
What is the main benefit of closed loop choke packets?
a) Reduced packet loss
b) Increased network capacity
c) Lower latency
d) Higher throughput
Which technique allows sources to adapt their transmission rates promptly based on explicit feedback?
a) Open loop choke packets
b) Closed loop choke packets
c) Dynamic routing
d) Quality of Service (QoS)
Which congestion control mechanism requires additional communication overhead?
a) Open loop choke packets
b) Closed loop choke packets
c) Dynamic routing
d) Quality of Service (QoS)
Which technique is more suitable for ensuring fairness in resource allocation?
a) Open loop choke packets
b) Closed loop choke packets
c) Dynamic routing
d) Quality of Service (QoS)
Which congestion control technique is commonly used in cloud data centers?
a) Open loop choke packets
b) Closed loop choke packets
c) Dynamic routing

d) Quality of Service (QoS)
What is the primary disadvantage of closed loop choke packets?
a) High implementation complexity
b) Increased packet loss
c) Unfair resource allocation
d) Limited control over congestion
Which mechanism allows routers to mark IP headers or TCP packets to indicate congestion levels?
a) Differentiated Services Code Points (DSCPs)
b) Explicit Congestion Notification (ECN)
c) TCP window size
d) Hop count
Which congestion control technique is based on open loop feedback?
a) Open loop choke packets
b) Closed loop choke packets
c) Dynamic routing
d) Quality of Service (QoS)
What is the purpose of Differentiated Services Code Points (DSCPs) in congestion control?
a) To mark packets with congestion levels
b) To indicate source IP addresses
c) To prioritize traffic based on application type
d) To measure network latency
Which congestion control mechanism allows for more efficient bandwidth allocation in real-time multimedia streaming?
a) Open loop choke packets
b) Closed loop choke packets
c) Dynamic routing
d) Quality of Service (QoS)

Conclusion of the Session

Congestion Control plays a vital role in managing network traffic and ensuring optimal performance. Two commonly used techniques for congestion control are open loop choke packets and closed loop choke packets.

Open loop choke packets allow routers to influence traffic sources directly without explicit feedback from the network. They achieve this by marking packets with Differentiated Services Code Points (DSCPs) to indicate congestion levels. Open loop choke packets provide simplicity and efficiency in congestion control but may have limited control over congestion.

Closed loop choke packets, on the other hand, provide more precise congestion feedback to traffic sources. They utilize mechanisms like Explicit Congestion Notification (ECN) to mark IP headers or TCP packets. Closed loop choke packets require bidirectional communication between routers and traffic sources, allowing for prompt adaptation of transmission rates based on explicit feedback. They are particularly effective in reducing packet loss and optimizing network performance.

Terminal Questions

Why does congestion occur?
Relate the congestion control and quality of service?
Illustrate traffic descriptor?
Compare the average data rate and the peak data rate?
Quote the definition of bursty data?
Compare the open-loop congestion control and closed-loop congestion control?
Categorize the policies that can prevent congestion.
Summarize the mechanisms that can alleviate congestion.
X=301, Since packets with sequence (301-400) is lost. After 3 duplicate acknowledgements (mild

congestion) -(301-400) will be send again.
Let the size of congestion window of a TCP connection be 32KB when a timeout occurs. The round trip time of the connection is 100msec and the maximum segment size used is 2KB. The time taken (in msec) by the TCP connection to get back to 32KB congestion window is?

Answers:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
c	a	b	b	b	b	a	a	b	a	a	b	b	b	a	a	b	a	c	b

Topic 6: QoS: Techniques to Improve QoS: Leaky bucket algorithm

QUALITY OF SERVICE:

In networking, a stream of packets sent from a source to a destination is typically referred to as a flow. The concept of flows is relevant in both connection-oriented and connectionless networks, but the behaviour of flows may differ between these network types. In a connection-oriented network, all packets belonging to a particular flow follow the same predetermined route. On the other hand, in a connectionless network, such as the Internet Protocol (IP) network, packets within a flow may take different routes. Each packet is independently routed across the network based on the network's routing protocols and policies. The needs of a flow, regardless of the network type, can be characterized by several primary parameters that determine the Quality of Service (QoS) requirements for that flow. These parameters include Reliability, Delay, Jitter and Bandwidth.

TECHNIQUES FOR ACHIEVING GOOD QOS:

1. Over provisioning
2. Buffering
3. Traffic shaping
    i. The leaky bucket algorithm
    ii. Token bucket algorithm
4. Packet scheduling
5. Admission control
6. Integrated services
    i. RSVP – Resource Reservation Protocol
7. Differentiated services
    i. Expedited forwarding

ii. Assured forwarding

OVERPROVISIONING:

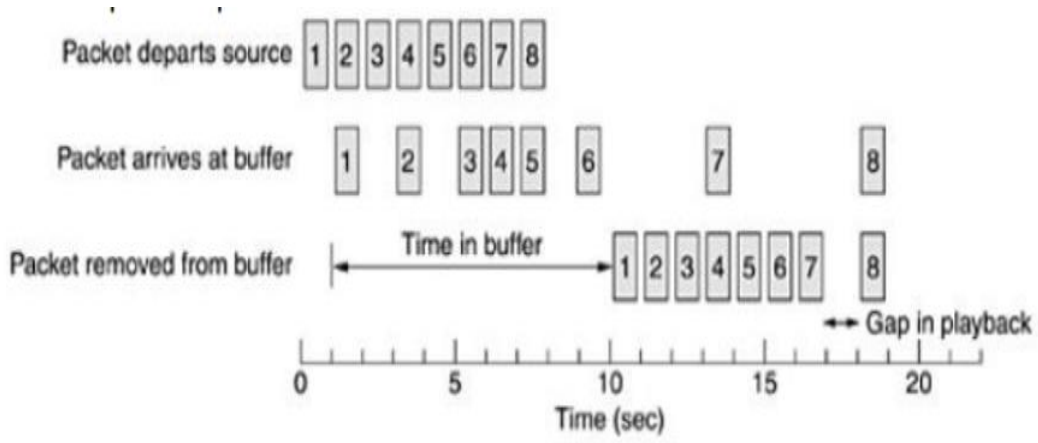
Overprovisioning in Quality of Service (QoS) refers to the practice of allocating more network resources than what is typically required to ensure that adequate bandwidth and other resources are available to meet the desired QoS objective. But the trouble with this method is that it is expensive.

BUFFERING:

Buffering is a fundamental technique used in Quality of Service (QoS) to manage and control network traffic, particularly in scenarios where there is a mismatch between the rate at which data is received and the rate at which it can be processed or transmitted.

In the context of QoS, buffering refers to the temporary storage of packets or data in a buffer or queue. When packets arrive at a network device, such as a router or switch, they are placed in a buffer before being processed or forwarded. The buffer acts as a temporary storage area that holds packets until they can be transmitted or further processed based on the defined QoS policies.

Buffering helps regulate the flow of traffic and plays a crucial role in managing network congestion, reducing packet loss, and ensuring a consistency quality of service.



TRAFFIC SHAPING:

Traffic shaping is a QoS Technique used to control the rate of network traffic flow, ensuring that it adheres to specific policies and limits. It is a proactive mechanism that regulates the transmission of packets based on predefined rules or shaping parameters.

The primary goal of traffic shaping is to smooth out bursts of traffic, prevent network congestion, and prioritize certain types of traffic over others. By controlling the rate at which packets are sent, traffic shaping helps achieve desired QoS objectives by allocating network resources appropriately.

Traffic shaping involves controlling the average rate of data transmission for a particular connection or circuit. When a connection is established between a user and the network subnet, they agree upon a specific traffic pattern or service level agreement (SLA) that outlines the expected behaviour and quality of service for that connection.

As long as the customer fulfils her part of the bargain and only sends packets according to the agreed-on contract, the carrier promises to deliver them all in a timely fashion.

Traffic shaping reduces congestion and thus helps the carrier live up to its promise. Such agreements are not so important for file transfers but are of great importance for real-time data, such as audio and video connections, which have stringent quality-of-service requirements.

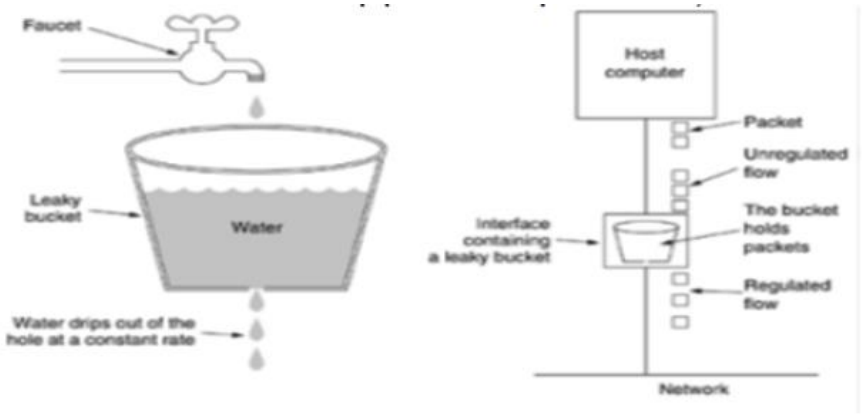
Monitoring a traffic flow is called traffic policing. Agreeing to a traffic shape and policing its afterward are easier with virtual-circuit subnets than with datagram subnets.

Leaky Bucket Algorithm:

The leaky bucket algorithm is a well-known traffic shaping mechanism used to control the rate at which packets or data are transmitted from a source. It is commonly used in network devices, such as routers or switches, to regulate outgoing traffic and ensure compliance with specified traffic contracts or quality of service (QoS) requirements.

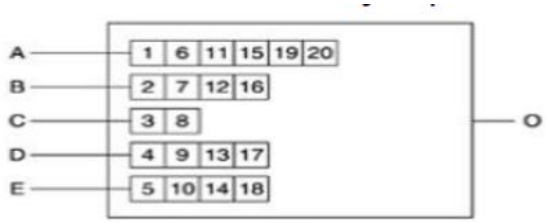
The concept of the leaky bucket algorithm can be visualized as a bucket with a leak. Incoming packets are considered as water drops that are poured into the bucket. The bucket has a fixed capacity or a predefined maximum burst size. If the bucket is full, any additional incoming packets are considered excess traffic and may be subject to different handling mechanisms, such as being dropped or marked.

The same idea can be applied to packets as shown in figure.



PACKET SCHEDULING:

Packet scheduling in QoS is a mechanism used to determine the order and timing of packet transmission in a network. It plays a crucial role in ensuring that various types of network traffic receive the appropriate level of service and resources based on their QoS requirements. If a router is handling multiple flows, there is a danger that one flow will take too much of its capacity and starve all the other flows. Packet scheduling algorithms can be devised to minimize it. One of the first ones was the fair queueing algorithm. The essence of the algorithm is that routers have separate queues for each output line, one for each flow. When a line becomes idle, the router scans the queues round robin, taking the first packet on the next queue. In this way, with n hosts competing for a given output line, each host gets to send one out of every n packets.



Packet	Finishing time
C	8
B	16
D	17
E	18
A	20

ADMISSION CONTROL:

Since many parties involved in the flow negotiation, flows must be described accurately in terms of specific parameters that can be negotiated. A set of such parameters is called flow specification. Typically, the sender produces a flow specification proposing the parameters it would like to use. As the specification propagates along the route, each router examines it and modifies the parameters as need be. The modifications can only reduce the flow, not increase it. When it gets to the other end, the parameters can be established. Consider an example of flow specification parameter for token bucket.

Parameter	Unit
Token bucket rate	Bytes/sec
Token bucket size	Bytes
Peak data rate	Bytes/sec
Minimum packet size	Bytes
Maximum packet size	Bytes

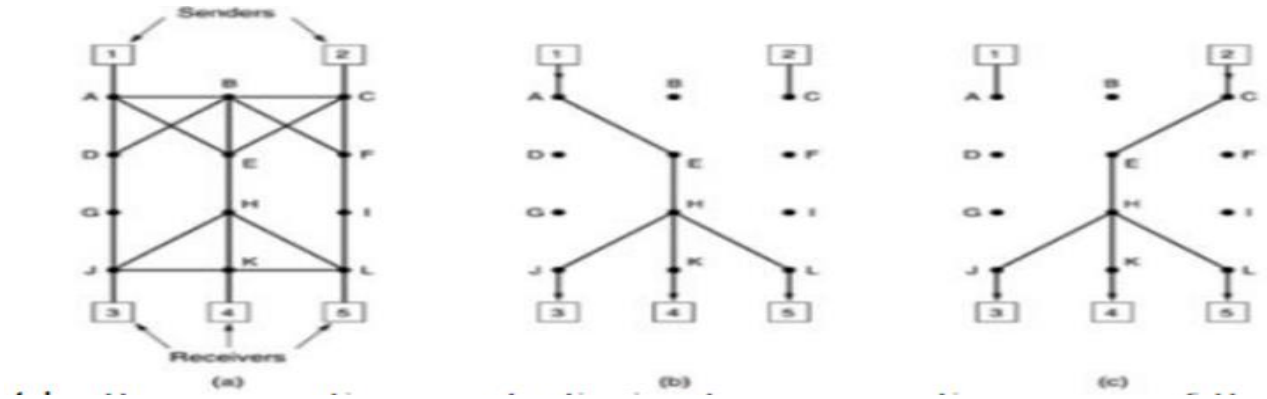
INTEGRATED SERVICES:

Flow-based algorithms or integrated services is aimed at providing QOS both unicast and multicast applications. An example of the unicast application is a single user streaming a video clip from a news site. An example of the latter is a collection of digital television stations broadcasting their programs as streams of IP packets to many receivers at various locations. Here we will concentrate on multicast, since unicast is a special case of multicast.

RSVP – Resource reSerVation Protocol:

The main protocol for integrated services architecture is RSVP. This protocol is used for making reservations. RSVP allows multiple senders to transmit to multiple groups of receivers, permits individual receivers to switch channels freely and optimizes bandwidth use while at the same time eliminating congestion. In its simplest form, the protocol uses multicast routing using spanning trees.

Each group is assigned a group address. To send to a group, a sender puts the group address in its packets. As an example, consider the network of Fig (a). Hosts 1 and 2 are multicast senders and hosts 3, 4 and 5 are multicast receivers. In this example, the senders and receivers are disjoint, but in general, the two sets may overlap. The multicast trees for hosts 1 and 2 are shown in Fig.(b) and Fig. (c) respectively.



To get better reception and eliminate congestion, any of the receivers in a group can send a reservation message up the tree to the sender. The message is propagated using the reverse path forwarding algorithm. At each hop, the router notes the reservation and reserves the necessary bandwidth. If insufficient bandwidth is available, it reports back failure. By the time the message gets back to the source, bandwidth has been reserved all the way from the sender to the receiver making the reservation request along the spanning tree.

DIFFERENTIATED SERVICES:

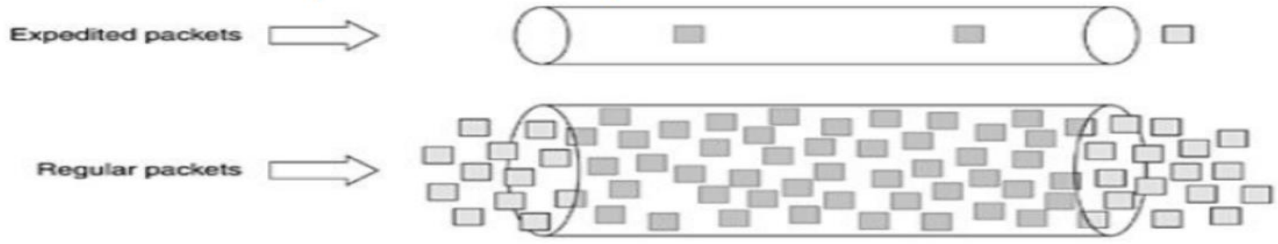
Flow-based algorithms have the potential to offer good QOS to one or more flows because they reserve whatever resources are needed along the route. They require an advanced set up to establish each flow, something that does not scale well when there are thousands or millions of flows. Also, they maintain internal per-flow state in the routers, making them vulnerable to router crashes.

For these reasons, a simpler approach is devised for QOS, one that can be largely implemented locally in each router without advance setup and without having the whole path involved. This approach is known as **class-based** QOS and the architecture is called **differentiated services.**

Differentiated services (DS) can be offered by a set of routers forming an administrative domain. The administration defines a set of service classes with corresponding forwarding rules. If a customer signs up for DS, customer packets entering the domain may carry a type of service field in them, with better service provided to some classes.

Expedited forwarding:

The choice of service classes is up to each operator, but since packets are often forwarded between subnets run by different operators, IETF (Internet Engineering Task Force) is working on defining network independent service classes. The simplest class is **expedited forwarding**. Two classes of service are available: regular and expedited. The vast majority of the traffic is expected to be regular, but a small fraction of the packets are expedited.

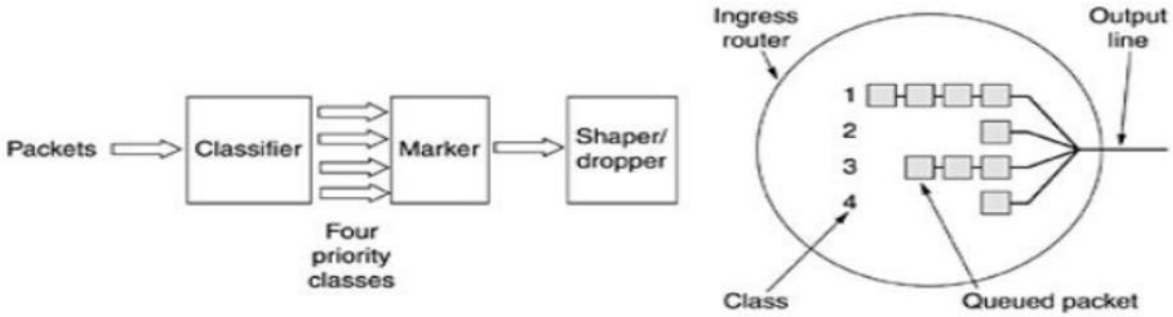


One way to implement this strategy is to program the routers to have two output queues for each outgoing line, one for expedited packets and one for regular packets. When a packet arrives, it is queued accordingly. Packet scheduling should use something like weighted fair queueing. For example, if 10% of the traffic is expedited and 90% is regular, 20% of the bandwidth could be dedicated to expedited traffic and the rest to regular traffic.

Doing so would give the expedited traffic twice as much bandwidth as it needs in order to provide low delay for it. This allocation can be achieved by transmitting one expedited packet for every four regular packets.

Assured forwarding:

A somewhat more elaborate scheme for managing the service classes is called assured forwarding. It specifies that there shall be four priority classes, each class having its own resources. In addition, it defines three discard probabilities for packets that are undergoing congestion: low, medium and high. Taken together, these two factors defines 12 service classes.



Step-1 is to classify the packets into one of the four priority classes. This step might be done on the sending host or in the ingress router. The advantage of doing classification on the sending host is that more information is available about which packets belong to which flows there. Step-2 is to mark the packets according to their class. A header field is needed for this purpose. Step-3 is to pass the packets through a shaper/dropper filter that may delay or drop some of them to shape the four streams into acceptable forms, for example, by using leaky or token buckets. If there are too many packets, some of them may be discarded here, by discard category.

SAQ's Self-Assessment Questions

In QOS, jitter is the variation in delay for packets belonging to
Same flow
Parallel flow
Protocol flow
Data flow
The token bucket can easily be implemented with a counter, initialized by?
0
1
-1
-2
In _____ congestion control, policies are applied to prevent congestion before it happens.
Open-loop
Closed-loop
Either A or B
Neither A nor B
In _____ congestion control, mechanisms are used to alleviate congestion after it happens.
Open-loop
Closed-loop
Either A or B
Neither A nor B
The technique of _____ refers to a congestion control mechanism in which a congested node stops

receiving data from the immediate upstream node or nodes.
Backpressure
Choke packet
Implicit signaling
Explicit signaling
A _____ is a packet sent by a node to the source to inform it of congestion.
Backpressure
Choke packet
Implicit signaling
Explicit signaling
In _____, there is no communication between the congested node or nodes and the source. The source guesses that there is a congestion somewhere in the network from other symptoms.
Backpressure
Choke packet
Implicit signaling
Explicit signaling
In the _____ method, the signal is included in the packets that carry data.
Backpressure
Choke packet
Implicit signaling
Explicit signaling
_____ is a characteristic that a flow needs. Lack of it means losing a packet or acknowledgement, which entails retransmission.
Reliability
Delay
Jitter
Bandwidth
_____ is a flow characteristic that applications can tolerate in different degrees.
Reliability
Delay
Jitter
Bandwidth
In _____, we try to avoid traffic congestion.
Congestion control
Quality of service
Both A and B
None of the above
In closed loop congestion control techniques, the decisions are based on the _____.
Concept of feedback loop
Concept of forward loop
Concept of current state of network
None of the above
The service of closed loop congestion control technique is _____.
When to accept new traffic
When to discard the packets
Monitor the system to detect when and where congestion occurs
Which packets to discard
The solution to increase the capacity when congestion occurs is _____.
Denying service to the users
Degrading the service to the users
Splitting traffic over multiple routes
Rescheduled the demans of the users
When too many packets are present in the subnet and performance degrades then it leads to _____.
Ingestion

Congestion
Digestion
Diffusion

For applications such as audio and video streaming, the variation in the packet arrival times is called _____.
Random early detection
Jitter
Delay difference
Load shedding

If the source deduces the existence of congestion by making local observations, such as the time needed for acknowledgements to come called as _____.
Explicit feedback algorithm
Implicit feedback algorithm
Explicit forward algorithm
Implicit forward algorithm

In open loop congestion control techniques, the decisions are based on the _____.
Without regard to the current state of the network
With regard to the current state of the network
With regard to the choice of the host
Without regard to the choice of the host

The solution to decrease the load on the network when congestion occurs is _____.
Splitting the traffic over multiple routes
Increasing the transmission power
Usage of spare routers
Denying service to the users

What is it goal of congestion control?
Making sure that subnet is not able to carry the offered traffic
Making sure that subnet will allow more than the offered packets
Making sure that subnet is able to carry the offered traffic
Making sure that subnet will not allow any traffic

Terminal Questions

What is Quality of service, and why is it important in networking?
Name the four parameters those can be used to characterize QOS?
What are different techniques used to prioritize traffic in QoS?
What is the disadvantage of Overprovisioning?
How buffering is used to avoid jitter problem in audio and video files?
What is service level agreement?
Define traffic policing in networking.

Summary

The average data rate, peak data rate, maximum burst size, and effective band width are qualitative values that describe a data flow.
A data flow can have a constant bit rate, a variable bit rate, or traffic that is bursty.
Qos in networking is a traffic control process that helps companies adjust their overall network traffic based on the requirements of specific time-sensitive applications.
It reduces common quality degradation issues such as packet loss, network jitter and high latency within the network.

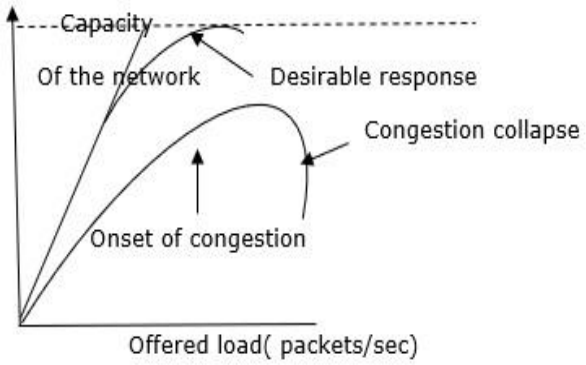
Answer Key:

A
A
A

B
A
B
C
D
A
B
A
A
C
C
B
B
B
A
D
C

Topic 7: Token bucket algorithm

The network layer and transport layer share the responsibility for handling congestions. One of the most effective ways to control congestion is trying to reduce the load that transport layer is placing on the network. To maintain this network and transport layers have to work together.



Token Bucket Algorithm

The leaky bucket algorithm enforces output patterns at the average rate, no matter how busy the traffic is. So, to deal with the more traffic, we need a flexible algorithm so that the data is not lost. One such approach is the token bucket algorithm.

Let us understand this algorithm step wise as given below −

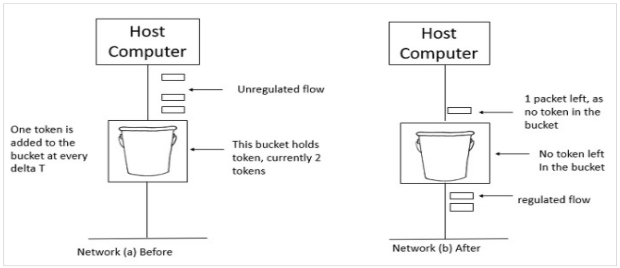
Step 1 − In regular intervals tokens are thrown into the bucket f.

Step 2 − The bucket has a maximum capacity f.

Step 3 − If the packet is ready, then a token is removed from the bucket, and the packet is sent.

Step 4 − Suppose, if there is no token in the bucket, the packet cannot be sent.

Let us understand the Token Bucket Algorithm with an example −



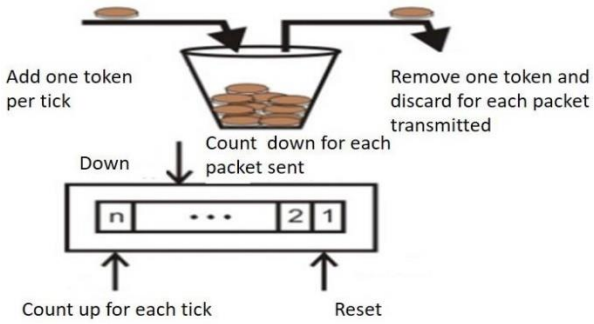
In figure (a) the bucket holds two tokens, and three packets are waiting to be sent out of the interface.

In Figure (b) two packets have been sent out by consuming two tokens, and 1 packet is still left.

When compared to Leaky bucket the token bucket algorithm is less restrictive that means it allows more traffic. The limit of busyness is restricted by the number of tokens available in the bucket at a particular instant of time.

The implementation of the token bucket algorithm is easy − a variable is used to count the tokens. For every t seconds the counter is incremented and then it is decremented whenever a packet is sent. When the counter reaches zero, no further packet is sent out.

This is shown in below given diagram −



Topic 8: ISNS Internet Storage Name Service

ISNS (Internet Storage name service)

Internet Storage Name Service brings the plug-and-play capabilities of Fibre Channel to IP storage networks.
Internet Storage Name Service brings the plug-and-play capabilities of Fibre Channel to IP storage networks. ISNS facilitates automated discovery, management, and configuration of iSCSI and Fibre Channel devices on a TCP/IP network. In a Fibre Channel fabric, a simple name server provides these services.
In any storage network, servers (or initiators) need to know which storage resources (or targets) they can access. One way to accomplish this is for an administrator to configure each initiator manually with its own list of authorized targets and configure each target with a list of authorized initiators and access controls. But this process is time-consuming and error-prone, and accidentally configuring multiple servers to access the same storage resources could be disastrous.
An Internet storage name server lets servers automatically identify and connect to authorized storage resources. Letting the servers dynamically adapt to changing storage resource membership and availability without human intervention results in even more efficiency.
Whereas a Fibre Channel storage name server can handle only Fibre Channel devices, iSNS can accommodate iSCSI devices and Fibre Channel devices via the Internet Fibre Channel Protocol. End nodes (initiators and targets) in an iSNS environment run a lightweight iSNS client that represents the host device to the iSNS server.
ISNS provides the following services:
Name registration and discovery services - Targets and initiators register their attributes and address, and then can obtain information about accessible storage devices dynamically.
Discovery domains and logon control service - Resources in a typical storage network are divided into groupings called discovery domains, which can be administered through network management applications. Discovery domains enhance security by providing access control to targets that are not enabled with their own access controls, while limiting the logon process of each initiator to a relevant subset of the available targets in the network.
State-change notification service - The iSNS server notifies relevant iSNS clients of network events that could affect the operational state of storage nodes. Events such as storage resources going offline, discovery domain membership changes and link failure in a network can trigger state-change notifications. These notifications let a network quickly adapt to changes in topology, which is key to scalability and availability.
Open mapping of Fibre Channel and iSCSI devices - The iSNS database can store information about Fibre Channel and iSCSI devices and mappings between the two in a multi-protocol environment. The mapped information is then available to any authorized iSNS client. This centralized approach is open and scalable instead of retrieving the mappings from individual iSCSI-FC gateways using proprietary mechanisms.
ISNS clients discover the iSNS server or servers using a variety of mechanisms, including Dynamic Host Configuration Protocol, Service Location Protocol and broadcast or multicast heartbeat messages. The iSNS framework allows for back-up iSNS servers that provide redundancy and

failover.
ISNS servers also can store and distribute X.509 public-key certificates used for authenticating iSCSI storage nodes during the logon process.
By facilitating a seamless integration of IP and Fibre Channel networks, iSNS provides value to any storage network composed of iSCSI and/or Fibre Channel devices. The iSNS specification is on the standards track with the Internet Engineering Task Force IP Storage Working Group and is expected to be classified as a proposed standard soon.

SAQ's Self-Assessment Questions

1. What does ISNS stand for?
   a) Internet Storage Name System
   b) Integrated Storage Networking Service
   c) Internet Storage Name Service
   d) Integrated Storage Name System
   Answer: c) Internet Storage Name Service

2. What is the primary purpose of ISNS?
   a) Dynamic configuration of storage devices
   b) Encryption of storage data
   c) Routing storage traffic
   d) Load balancing in storage networks
   Answer: a) Dynamic configuration of storage devices

3. Which protocol is commonly used by ISNS for communication?
   a) FTP (File Transfer Protocol)
   b) NFS (Network File System)
   c) SNMP (Simple Network Management Protocol)
   d) TCP/IP (Transmission Control Protocol/Internet Protocol)
   Answer: d) TCP/IP (Transmission Control Protocol/Internet Protocol)

4. What is the role of ISNS in storage resource discovery?
   a) Assigning IP addresses to storage devices
   b) Managing storage device access control
   c) Providing centralized storage resource information
   d) Encrypting storage data during transmission
   Answer: c) Providing centralized storage resource information

5. Which component of ISNS maintains a database of storage devices and services?
   a) ISNS Name Server
   b) ISNS Management Agent
   c) ISNS Discovery Service
   d) ISNS Access Control List
   Answer: a) ISNS Name Server

6. What is the purpose of an ISNS Discovery Service?
   a) Authenticating storage devices
   b) Discovering storage devices in the network
   c) Assigning unique names to storage devices
   d) Managing storage access permissions
   Answer: b) Discovering storage devices in the network

7. Which ISNS component provides management and control functions for ISNS operation?
   a) ISNS Name Server

b) ISNS Management Agent
c) ISNS Discovery Service
d) ISNS Access Control List
Answer: b) ISNS Management Agent

8. How does ISNS handle storage device naming?
a) Using MAC addresses for naming
b) Utilizing DNS (Domain Name System) for naming
c) Assigning unique names using ISNS protocol
d) Based on the manufacturer's naming convention
Answer: c) Assigning unique names using ISNS protocol

9. Which security mechanism is commonly employed by ISNS for secure communication?
a) SSH (Secure Shell)
b) SSL/TLS (Secure Sockets Layer/Transport Layer Security)
c) IPSec (Internet Protocol Security)
d) SNMPv3 (Simple Network Management Protocol version 3)
Answer: b) SSL/TLS (Secure Sockets Layer/Transport Layer Security)

10. Which protocol is used by ISNS to register and deregister storage devices?
a) LDAP (Lightweight Directory Access Protocol)
b) DHCP (Dynamic Host Configuration Protocol)
c) ICMP (Internet Control Message Protocol)
d) iSNS (Internet Storage Name Service) Protocol
Answer: d) iSNS (Internet Storage Name Service) Protocol

11. How does ISNS facilitate dynamic configuration of storage devices?
a) By automatically assigning IP addresses to devices
b) By providing a web-based management interface
c) By using SNMP for device configuration
d) By exchanging control messages with storage devices
Answer: d) By exchanging control messages with storage devices

12. Which ISNS functionality allows for automated load balancing in storage networks?
a)

Path discovery
b) Resource enumeration
c) Service advertisement
d) Access control
Answer: a) Path discovery

13. What is the purpose of ISNS access control lists (ACLs)?
a) To restrict access to storage resources
b) To filter network traffic in storage networks
c) To assign IP addresses to storage devices
d) To configure VLANs (Virtual Local Area Networks)
Answer: a) To restrict access to storage resources

14. How does ISNS support failover and redundancy in storage networks?
a) By providing backup storage services
b) By utilizing multipath I/O (Input/Output) techniques
c) By implementing RAID (Redundant Array of Independent Disks)
d) By integrating with network load balancers

Answer: b) By utilizing multipath I/O (Input/Output) techniques

15. Which ISNS component handles queries and responses for storage resource information?
a) ISNS Name Server
b) ISNS Management Agent
c) ISNS Discovery Service
d) ISNS Access Control List
Answer: a) ISNS Name Server

16. What type of information can be stored in an ISNS database?
a) Storage device model numbers
b) Storage device serial numbers
c) Storage service locations
d) All of the above
Answer: d) All of the above

17. Which ISNS feature provides notifications about changes in storage resource availability?
a) Registration
b) Enumeration
c) Notifications
d) Discovery
Answer: c) Notifications

18. How does ISNS handle name conflicts in storage networks?
a) It assigns additional attributes to resolve conflicts
b) It assigns different IP addresses to devices with the same name
c) It provides error messages to administrators for manual resolution
d) It automatically resolves conflicts based on time of registration
Answer: a) It assigns additional attributes to resolve conflicts

19. Which ISNS functionality provides a mechanism for managing storage device access permissions?
a) Authentication
b) Authorization
c) Auditing
d) Accounting
Answer: b) Authorization

20. Which industry standard defines the ISNS protocol?
a) RFC 3720
b) RFC 1918
c) RFC 3986
d) RFC 2821
Answer: a) RFC 3720

Terminal Questions:

1. What is ISNS (Internet Storage Name Service), and what is its role in storage networking?
2. How does ISNS facilitate storage resource discovery and management in a network environment?
3. What are the benefits of using ISNS in a storage network compared to other management protocols?
4. How does ISNS handle naming and addressing of storage devices and services?
5. What security measures are implemented in ISNS to protect the storage network from unauthorized access and potential threats?

Topic 9: Presentation Layer: Preface of Socket,Secure Socket Layer

Preface to the Socket

Sockets in computer networks are used for allowing the transmission of information between two processesof the same machines or different machines in the network. The socket is the combination of IP address and software port number used for communication between multiple processes. Socket helps to recognize the address of the application to which data is to be sent using the IP address and port number.

Sockets allow communication of two processes that are running on the same or different machines.

Socketsare the end of two-way communication between two programs that are running on the networks.

Sockets are mostly used in client-server architecture for communication between multiple applications.

The socket is created by the combination of the IP address and port number of the software. With this combination, the process knows the system address and address of the application where datais to be sent

Types of Sockets:

There are two types of Sockets: the datagram socket and the stream socket.

Datagram Socket: This is a type of network which has connection less point for sending and receiving packets. It is similar to mailbox. The letters (data) posted into the box are collected and delivered (transmitted) to a letterbox (receiving socket).

Stream Socket: In Computer operating system, a stream socket is type of inter-process communications socket or network socket which provides a connection-oriented, sequenced, and unique flow of data without record boundaries with well-defined mechanisms for creating and destroying connections and for detecting errors. It is similar to phone. A connection is established between the phones (two ends) and a conversation (transfer of data) takes place.

Secure Socket Layer

SSL, or Secure Sockets Layer, is an encryption-based Internet security protocol. It was first developed by Netscape in 1995 for the purpose of ensuring privacy, authentication, and data integrity in Internet communications. SSL is the predecessor to the modern TLS encryption used today.

A website that implements SSL/TLS has "HTTPS" in its URL instead of "HTTP."

Versions of SSL:

SSL 1 – Never released due to high insecurity.
SSL 2 – Released in 1995.
SSL 3 – Released in 1996.
TLS 1.0 – Released in 1999.
TLS 1.1 – Released in 2006.
TLS 1.2 – Released in 2008.
TLS 1.3 – Released in 2018

Working of SSL

In order to provide a high degree of privacy, SSL encrypts data that is transmitted across the web. This means that anyone who tries to intercept this data will only see a garbled mix of characters that is nearly impossible to decrypt.

SSL initiates an authentication process called a handshake between two communicating devices to ensure that both devices are really who they claim to be.

SSL also digitally signs data in order to provide data integrity, verifying that the data is not tampered with before reaching its intended recipient.

There have been several iterations of SSL, each more secure than the last. In 1999 SSL was updated to become TLS.
Secure Socket Layer Protocols:
SSL record protocol
Handshake protocol
Change-cipher spec protocol
Alert protocol

Characteristics of SSL Certificate

The SSL certificate has several important characteristics that make it a reliable solution for securing online transactions:

Encryption: The SSL certificate uses encryption algorithms to secure the communication between the website or service and its users. This ensures that the sensitive information, such as login credentials and credit card information, is protected from being intercepted and read by unauthorized parties.

Authentication: The SSL certificate verifies the identity of the website or service, ensuring that users are communicating with the intended party and not with an impostor. This provides assurance to users that their information is being transmitted to a trusted entity.

Integrity: The SSL certificate uses message authentication codes (MACs) to detect any tampering with the data during transmission. This ensures that the data being transmitted is not modified in any way, preserving its integrity.

Non-repudiation: SSL certificates provide non-repudiation of data, meaning that the recipient of the data cannot deny having received it. This is important in situations where the authenticity of the information needs to be established, such as in e-commerce transactions.

Public-key cryptography: SSL certificates use public-key cryptography for secure key exchange between the client and server. This allows the client and server to securely exchange encryption keys, ensuring that the encrypted information can only be decrypted by the intended recipient.

Session management: SSL certificates allow for the management of secure sessions, allowing for the resumption of secure sessions after interruption. This helps to reduce the overhead of establishing a new secure connection each time a user accesses a website or service.

Certificates issued by trusted CAs: SSL certificates are issued by trusted CAs, who are responsible for verifying the identity of the website or service before issuing the certificate. This provides a high level of trust and assurance to users that the website or service they are communicating with is authentic and trustworthy.

In addition to these key characteristics, SSL certificates also come in various levels of validation, including Domain Validation (DV), Organization Validation (OV), and Extended Validation (EV). The level of validation determines the amount of information that is verified by the CA before issuing the certificate, with EV certificates providing the highest level of assurance and trust to users.

Terminal Questions

What Is Server Socket Class?
What Is Socket Class?
Explain What Is SSL?
Tell Me How Do Sockets Work?

Summary

The SSL certificate is an important component of online security, providing encryption, authentication, integrity, non-repudiation, and other key features that ensure the secure and reliable transmission of sensitive information over the internet.

Topic 10: TELNET, TFTP, POP3

TELNET

TELNET stands for Teletype Network. It is a type of protocol that enables one computer to connect to the local computer. It is used as a standard TCP/IP protocol for virtual terminal service which is provided by ISO. The computer which starts the connection is known as the local computer.

The computer which is being connected to i.e. which accepts the connection known as the remote computer.

During telnet operation, whatever is being performed on the remote computer will be displayed by the local computer. Telnet operates on a client/server principle. The local computer uses a telnet client program and the remote computers use a telnet server program.

Logging:

The logging process can be further categorized into two parts:

Local Login

Remote Login

1. Local Login: Whenever a user logs into its local system, it is known as local login.

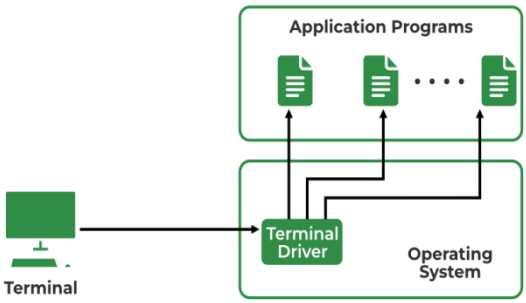


Fig: 10.1 TELNET Connectivity

The Procedure of Local Login

Keystrokes are accepted by the terminal driver when the user types at the terminal.

Terminal Driver passes these characters to OS.

Now, OS validates the combination of characters and opens the required application.

2. Remote Login: Remote Login is a process in which users can log in to a remote site i.e. computer and use services that are available on the remote computer. With the help of remote login, a user is able to understand the result of transferring the result of processing from the remote computer to the local computer.

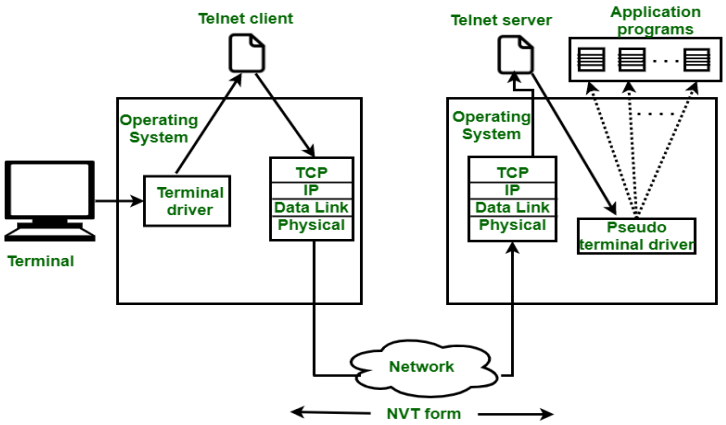


Fig 10.2: Remote Login

The Procedure of Remote Login

When the user types something on the local computer, the local operating system accepts the character.

The local computer does not interpret the characters, it will send them to the TELNET client.

TELNET client transforms these characters to a universal character set called Network Virtual Terminal (NVT) characters and it will pass them to the local TCP/IP protocol Stack.

Commands or text which are in the form of NVT, travel through the Internet and it will arrive at the TCP/IP stack at the remote computer.

Characters are then delivered to the operating system and later on passed to the TELNET server.

Then TELNET server changes those characters to characters that can be understandable by a remote computer.

The remote operating system receives characters from a pseudo-terminal driver, which is a piece of software that pretends that characters are coming from a terminal.

The operating system then passes the character to the appropriate application program.

TFTP:

TFTP stands for Trivial File Transfer Protocol. It is a simplified version of the File Transfer Protocol (FTP) that is used primarily for transferring files between network devices. TFTP operates at the Application Layer of the TCP/IP protocol suite.

TFTP is often used in scenarios where a device, such as a router or a switch, needs to retrieve or update firmware or configuration files from a central server. It is a lightweight protocol that requires minimal resources, making it suitable for devices with limited memory or processing capabilities.

Key features of TFTP include:

Simplicity: TFTP has a minimal set of commands and features compared to FTP. It uses a simple request-response model for file transfers.

UDP-based: TFTP uses User Datagram Protocol (UDP) as the transport protocol instead of Transmission Control Protocol (TCP). UDP is connectionless and provides less overhead, but it does not guarantee reliable data delivery.

No authentication: TFTP does not provide built-in authentication mechanisms. It typically relies on other protocols, such as DHCP (Dynamic Host Configuration Protocol), to obtain network configuration details.

Read and write operations: TFTP supports two basic operations: Read (RRQ) and Write (WRQ). A client initiates a Read request to retrieve a file from the server, while a Write

request is used to upload a file to the server.
TFTP does not include features like directory listings, file deletion, or file renaming, which are available in more comprehensive file transfer protocols like FTP or SCP (Secure Copy Protocol). Its simplicity and limited feature set make it suitable for specific use cases where a basic, lightweight file transfer mechanism is required.
However, it's worth noting that TFTP, like TELNET, sends data in plain text without encryption, which means it is also considered insecure for transferring sensitive or confidential data. For secure file transfers, protocols like SCP, SFTP (SSH File Transfer Protocol), or HTTPS (HTTP Secure) are commonly used.

POP3:
POP3 stands for Post Office Protocol version 3. It is a standard Internet protocol used for receiving email messages from a mail server to a client device, such as a computer or a mobile device. POP3 is one of the most commonly used protocols for email retrieval.
Here's how POP3 works:
Connection establishment: The client establishes a TCP/IP connection with the mail server on the well-known port 110.
Authentication: The client provides its username and password to authenticate itself to the mail server. This step ensures that only authorized users can access their email accounts.
Mailbox access: Once authenticated, the client can issue commands to access and manage email messages stored on the server. Common commands include retrieving email, marking messages as read or deleted, listing the number of messages, and deleting messages.
Message retrieval: The client can use the "RETR" command to retrieve individual email messages from the server. The server sends the requested message(s) to the client over the established connection.
Message deletion: When a client deletes a message, it is marked for deletion on the server. However, the actual deletion occurs during the "QUIT" command, which closes the POP3 session. Marked-for-deletion messages are removed from the server at that time.
Session termination: The client issues the "QUIT" command to terminate the POP3 session. The server acknowledges the termination, and the connection is closed.
Unlike more modern protocols such as IMAP (Internet Message Access Protocol), which allows users to access their email messages while leaving them stored on the server, POP3 typically downloads email messages to the client device, removing them from the server by default. However, some POP3 clients provide options to leave a copy of the messages on the server for a specified period or under certain conditions.
It's worth noting that POP3 does not support two-way synchronization, meaning actions performed on the client (such as marking messages as read or deleting them) are not reflected on the server or other connected devices. If you need to access your email from multiple devices and keep them in sync, IMAP is generally a more suitable protocol.

SAQ's-Self Assessment Questions

1. Telnet protocol is used to establish a connection to _____
a. TCP port number 21
b. TCP port number 22
c. TCP port number 23
d. TCP port number 25
Answer: c
2. Which one of the following is not correct?
a. telnet is a general-purpose client-server program

b. telnet lets user access an application on a remote computer
c. telnet can also be used for file transfer
d. telnet can be used for remote login
Answer: c
3. What is the full form of TFTP?
a. Transmission File Transfer Protocol
b. Trivial File Transfer Protocol
c. Transport File Transfer Protocol
d. None of the above
Answer: b
4. POP3 is an email-related protocol. What does the numeric value '3' in POP3 represent?
a. Number of characters in POP
b. Header size of POP
c. Version of POP
d. Number of codes in POP
Answer: c
5. Post Office Protocol is a ---------.
a. Connection-oriented protocol
b. Connectionless protocol
c. Stateless protocol
d. None of the above
Answer: a
6. Which one of the following is not true?
a. telnet defines a network virtual terminal (NVT) standard
b. client programs interact with NVT
c. server translates NVT operations
d. client can transfer files using to remote server using NVT
Answer: d
7. All telnet operations are sent as _____
a. 4 bits
b. 8 bits
c. 16 bits
d. 32 bits
Answer: b
8. The application layer protocol used by a Telnet application is _____
a. Telnet
b. FTP
c. HTTP
d. SMTP
Answer: a
9. _____ allows you to connect and login to a remote computer
a. Telnet
b. FTP
c. HTTP
d. SMTP
Answer: a
10. Telnet is used for _____
a. Television on net
b. Network of Telephones
c. Remote Login

d. Teleshopping site
Answer: c
11. Which information form/type is used for transferring the data in Packet switching?
a. Morse
b. ASCII
c. Binary
d. Baudot
Answer: c
12. If the sender wants an option enabled by the receiver, it sends a ____ command?
a. will
b. do
c. wont
d. none of the above
Answer: b
13. _____ is the standard mechanism provided by TCP/IP for copying a file from one host to another.
a. TELNET
b. SMTP
c. TFTP
d. None of the above
Answer: d
14. FTP uses the services of _____.
a. UDP
b. TCP
c. IP
d. none of the above
answer: b
15. In FTP, the well-known port _____ is used for the control connection and the well-known port _____ for the data connection.
a. 21; 22
b. 21; 20
c. 20; 21
d. none of the above
answer: b
16. In FTP, _____ is the service type used by the IP protocol because this is an interactive connection between a user and a server.
a. maximize throughput
b. minimize error
c. minimize delay
d. none of the above
answer: c
17. Which of the following is not a secured mail transferring methodology?
a. POP3
b. SSMTP
c. Mail using PGP
d. S/MIME
answer: a
18. During an FTP session the data connection is opened _____.
a. exactly once
b. exactly twice

c. as many times as necessary
d. none of the above
answer: c
19. During an FTP session the control connection is opened _____.
a. exactly once
b. exactly twice
c. as many times as necessary
d. none of the above
answer: a
20. In FTP, when we _____, it is copied from the server to the client.
a. retrieves a file
b. retrieves a list
c. a and c
d. none of the above
answer: c

Terminal Questions

What is TELNET? And What it is used for?
How do you establish a TELNET connection to a remote server?
How does TELNET differ from SSH?
What is POP3 and how does it work?
What are the advantages of using POP3 for email retrieval?
Can POP3 be used for sending email, or is it only for receiving email?
What is TFTP and what is its purpose?

Topic 11: SNMP, E-mail-SMTP

SNMP (Simple Network Management Protocol)
Simple Network Management Protocol (SNMP) is an application-layer protocol for monitoring and managing network devices on a local area network (LAN) or wide area network (WAN).
The purpose of SNMP is to provide network devices, such as routers, servers and printers, with a common language for sharing information with a network management system (NMS). The SNMP manager acts as the client, the SNMP agent acts as the server and the MIB acts as the server's database. When the SNMP manager asks the agent a question, the agent uses the MIB to supply the answer.
SNMP is part of the original Internet Protocol (IP) suite as defined by the Internet Engineering Task Force (IETF). Multiple versions of the SNMP protocol exist. The most recent version, SNMPv3, includes security mechanisms for authentication, encryption and access control.
SNMP Concept

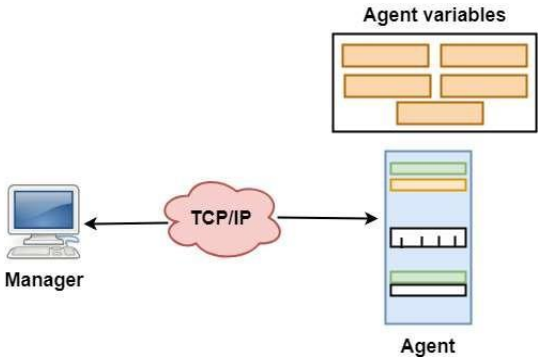


Fig: 11.1 SNMP Concept

SNMP has two components Manager and agent.
The manager is a host that controls and monitors a set of agents such as routers.
It is an application layer protocol in which a few manager stations can handle a set of agents.
The protocol designed at the application level can monitor the devices made by different manufacturers and installed on different physical networks.
It is used in a heterogeneous network made of different LANs and WANs connected by routers or gateways.

Managers & Agents
A manager is a host that runs the SNMP client program while the agent is a router that runs the SNMP server program.
Management of the internet is achieved through simple interaction between a manager and agent. The agent is used to keep the information in a database while the manager is used to access the values in the database. For example, a router can store the appropriate variables such as a number of packets received and forwarded while the manager can compare these variables to determine whether the router is congested or not.
Agents can also contribute to the management process. A server program on the agent checks the environment, if something goes wrong, the agent sends a warning message to the manager.

Management with SNMP has three basic ideas:
A manager checks the agent by requesting the information that reflects the behavior of the agent.
A manager also forces the agent to perform a certain function by resetting values in the agent database.
An agent also contributes to the management process by warning the manager regarding an unusual condition.

Management Components
Management is not achieved only through the SNMP protocol but also the use of other protocols that can cooperate with the SNMP protocol. Management is achieved through the use of the other two protocols: SMI (Structure of management information) and MIB(management information base). Management is a combination of SMI, MIB, and SNMP. All these three protocols such as abstract syntax notation 1 (ASN.1) and basic encoding rules (BER).

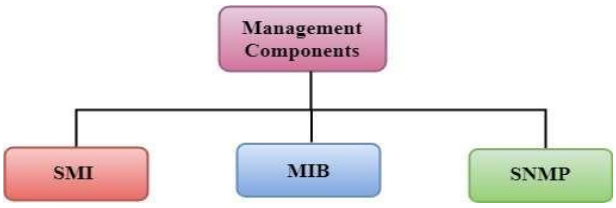


Fig 11.2: SNMP Management Components

SMI
The SMI (Structure of management information) is a component used in network management. Its main function is to define the type of data that can be stored in an object and to show how to encode the data for the transmission over a network.
MIB
The MIB (Management information base) is a second component for the network management. Each agent has its own MIB, which is a collection of all the objects that the manager can manage. MIB is categorized into eight groups: system, interface, address translation, ip, icmp, tcp, udp, and egp. These groups are under the mib object.
SNMP
SNMP defines five types of messages: GetRequest, GetNextRequest, SetRequest, GetResponse, and Trap.

GetRequest: The GetRequest message is sent from a manager (client) to the agent (server) to retrieve the value of a variable.

GetNextRequest: The GetNextRequest message is sent from the manager to agent to retrieve the value of a variable. This type of message is used to retrieve the values of the entries in a table. If the manager does not know the indexes of the entries, then it will not be able to

retrieve the values. In such situations, GetNextRequest message is used to define an object.

GetResponse: The GetResponse message is sent from an agent to the manager in response to the GetRequest and GetNextRequest message. This message contains the value of a variable requested by the manager.

SetRequest: The SetRequest message is sent from a manager to the agent to set a value in a variable.

Trap: The Trap message is sent from an agent to the manager to report an event. For example, if the agent is rebooted, then it informs the manager as well as sends the time of rebooting.

EMAIL (SMTP, MIME, IMAP, POP)
One of the most popular Internet services is electronic mail (E-mail).
Email is one of the oldest network applications.
The three main components of an Email are
User Agent (UA)
Message Transfer Agent (MTA) – SMTP
Message Access Agent (MAA) - IMAP, POP
When the sender and the receiver of an e-mail are on the same system, we needonlytwo User Agents and no Message Transfer Agent
When the sender and the receiver of an e-mail are on different system, we need twoUA, two pairs of MTA (client and server), and two MAA (client and server).

USER AGENT (UA)
The first component of an electronic mail system is the user agent (UA).
It provides service to the user to make the process of sending and receiving amessage easier.
A user agent is a software package that composes, reads, replies to, andforwardsmessages. It also handles local mailboxes on the user computers.

MESSAGE TRANSFER AGENT (MTA)
The actual mail transfer is done through message transfer agents (MTA).
To send mail, a system must have the client MTA, and to receive mail, asystemmust have a server MTA.

The formal protocol that defines the MTA client and server in the Internet iscalledSimple Mail Transfer Protocol (SMTP).

MESSAGE ACCESS AGENT (MAA)
MAA is a software that pulls messages out of a mailbox.
POP3 and IMAP4 are examples of MAA.

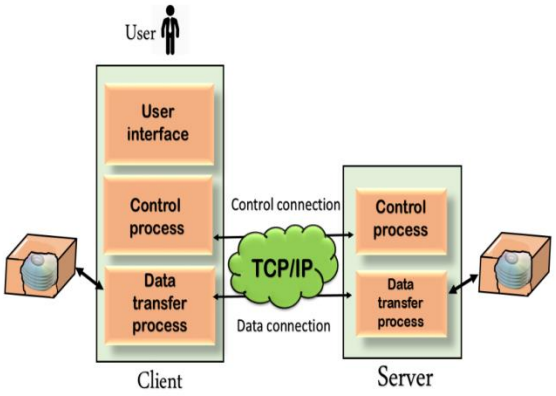
SIMPLE MAIL TRANSFER PROTOCOL (SMTP)

SMTP is the standard protocol for transferring mail between hosts in theTCP/IPprotocol suite.
SMTP is not concerned with the format or content of messages themselves.
SMTP uses information written on the *envelope* of the mail (message header),butdoes not look at the *contents* (message body) of the envelope.

Topic 12: FTP, NTP, SSDP

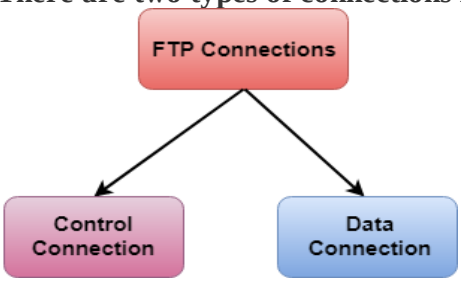
FTP (File Transfer Protocol)
Although transferring files from one system to another is very simple and straightforward, but sometimes it can cause problems. For example, two systems may have different file conventions. Two systems may have different ways to represent text and data. Two systems may have different directory structures. FTP protocol overcomes these problems by establishing two connections between hosts. One connection is used for data transfer, and another connection is used for the control connection.

Mechanism of FTP



The above figure shows the basic model of the FTP. The FTP client has three components: the user interface, control process, and data transfer process. The server has two components: the server control

process and the server data transfer process.
There are two types of connections in FTP:



Control Connection: The control connection uses very simple rules for communication. Through control connection, we can transfer a line of command or line of response at a time. The control connection is made between the control processes. The control connection remains connected during the entire interactive FTP session.
Data Connection: The Data Connection uses very complex rules as data types may vary. The data connection is made between data transfer processes. The data connection opens when a command comes for transferring the files and closes when the file is transferred.
FTP Clients
FTP client is a program that implements a file transfer protocol which allows you to transfer files between two hosts on the internet.
It allows a user to connect to a remote host and upload or download the files.
It has a set of commands that we can use to connect to a host, transfer the files between you and your host and close the connection.
The FTP program is also available as a built-in component in a Web browser. This GUI based FTP client makes the file transfer very easy and also does not require to remember the FTP commands.
Advantages of FTP:
Speed: One of the biggest advantages of FTP is speed. FTP is one of the fastest way to transfer the files from one computer to another computer.
Efficient: It is more efficient as we do not need to complete all the operations to get the entire file.
Security: To access the FTP server, we need to login with the username and password. Therefore, we can say that FTP is more secure.
Back & forth movement: FTP allows us to transfer the files back and forth. Suppose you are a manager of the company, you send some information to all the employees, and they all send information back on the same server.
Disadvantages of FTP:
The standard requirement of the industry is that all the FTP transmissions should be encrypted. However, not all the FTP providers are equal and not all the providers offer encryption. So, we will have to look out for the FTP providers that provide encryption.
FTP serves two operations, i.e., to send and receive large files on a network. However, the size limit of the file is 2GB that can be sent. It also doesn't allow you to run simultaneous transfers to multiple receivers.
Passwords and file contents are sent in clear text that allows unwanted eavesdropping. So, it is quite possible that attackers can carry out the brute force attack by trying to guess the FTP password.
It is not compatible with every system.

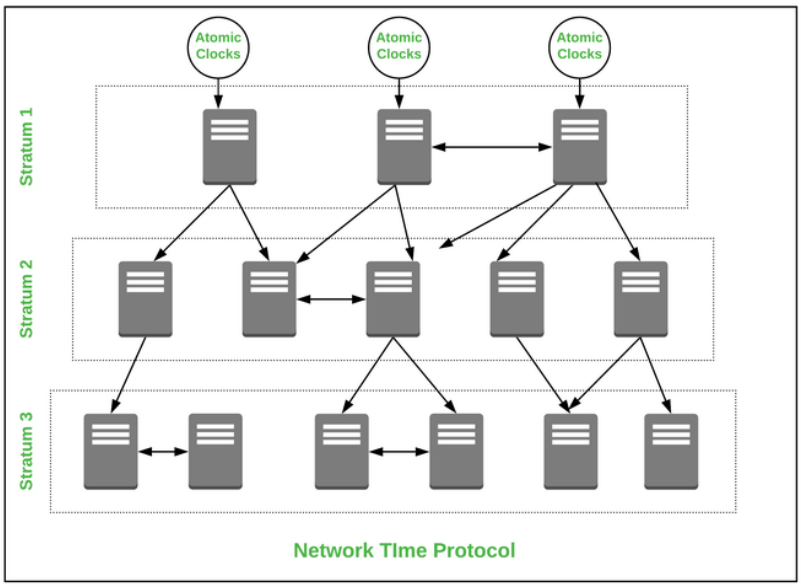
NTP
Network Time Protocol (NTP) is a protocol that helps the computers clock times to be synchronized in a network. This protocol is an application protocol that is responsible for the synchronization of hosts on a TCP/IP network. NTP was developed by David Mills in 1981 at the University of Delaware. This is required in a communication mechanism so that a seamless connection is present between the computers.
Features of NTP:
Some features of NTP are –
NTP servers have access to highly precise atomic clocks and GPU clocks.

It uses Coordinated Universal Time (UTC) to synchronize CPU clock time.
Avoids even having a fraction of vulnerabilities in information exchange communication.
Provides consistent timekeeping for file servers.

Working of NTP:

NTP is a protocol that works over the application layer, it uses a hierarchical system of time resources and provides synchronization within the stratum servers. First, at the topmost level, there is highly accurate time resources' ex. atomic or GPS clocks. These clock resources are called stratum 0 servers, and they are linked to the below NTP server called Stratum 1,2 or 3 and so on. These servers then provide the accurate date and time so that communicating hosts are synced to each other.

Architecture of Network Time Protocol:



Applications of NTP:

Used in a production system where the live sound is recorded.
Used in the development of Broadcasting infrastructures.
Used where file system updates needed to be carried out across multiple computers depending on synchronized clock times.
Used to implement security mechanisms which depend on consistent time keeping over the network.
Used in network acceleration systems which rely on timestamp accuracy to calculate performance.

Advantages of NTP:

It provides internet synchronization between the devices.
It provides enhanced security within the premises.
It is used in authentication systems like Kerberos.
It provides network acceleration which helps in troubleshooting problems.
Used in file systems that are difficult in network synchronization.

Disadvantages of NTP:

When the servers are down the sync time is affected across a running communication.
Servers are prone to error due to various time zones and conflict may occur.
Minimal reduction of time accuracy.
When NTP packets are increased synchronization is conflicted.
Manipulation can be done in synchronization.

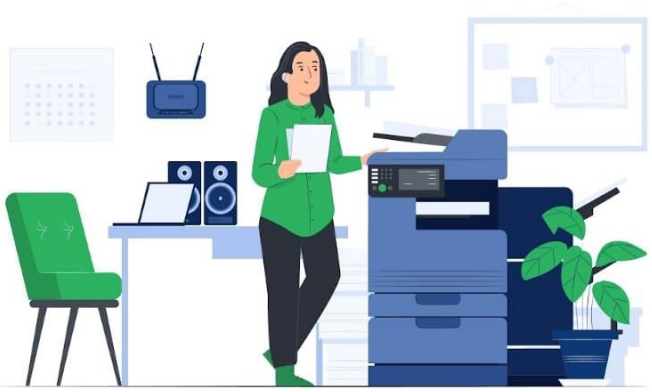
SSDP (Simple Service Discovery Protocol)

SSDP (Simple Service Discovery Protocol) is a network protocol used in small networks, including home networks, to advertise and discover network services primarily supported by the Universal Plug-and-Play (UPnP) architecture. SSDP is an HTTPU-based textual protocol that uses XML. It exchanges messages using UDP datagrams.

Easy to set up:

SSDP is the backbone of the UPnP architecture. It allows you to easily interconnect home devices that work within the same small network or connected to the same Wi-Fi point. Such devices may include,

for example, smartphones, printers and MFPs, smart TVs, media consoles, speakers, camcorders, etc. For SSDP to work, these devices must support UPnP.
On devices and PCs that support SSDP, this feature can be enabled, disabled, or paused. When SSDP is enabled, devices communicate information about themselves and the services they provide to any other UPnP client. Using SSDP, computers connected to the network also provide information about available services.



Using SSDP, devices and PCs not only learn about each other, but also get the opportunity to interact in some way: exchange data, launch functions and services on another device, etc.

Threats associated with SSDP:

From the point of view of information security, you need to remember that, firstly, the SSDP protocol itself does not provide encryption (although, of course, it does not prevent devices from exchanging encrypted data), and, secondly, in many devices intended for use in home in a small office environment, SSDP support is enabled by default, posing risks of unauthorized access. Therefore, this feature should be kept disabled: enable it only when you really need it, and make sure that it is disabled on each of the devices that are not currently using it.
You can check if the SSDP discovery service is enabled on your Windows PC using the services.msc command. To make sure that SSDP support is enabled on a particular device, you should carefully study the instructions for it and check the settings.
It should also be remembered that SSDP features are used in the implementation of DDoS attacks such as "SSDP amplification".

DDoS attacks using SSDP:

These types of network layer (L3) attacks exploit the vulnerabilities of the SSDP protocol, which are embedded in it, probably out of the desire of its developers to simplify the interaction of devices in a small network as much as possible. Unfortunately, this simplicity comes at the expense of security.
In its most general form, the connection of a new device looks like this. To find out which devices are already present on the network, a device added to it with SSDP enabled sends a search request to other devices to the reserved address and port (239.255.255.250:1900), using fan-out or multicasting. In the request, the device specifies a template or target corresponding to its type. In response to the request, each of the devices on the network that support SSDP at the moment sends a UDP message with information about itself to the source IP address and port from which the request was sent.
The trick is that within the SSDP protocol, the location of the message sender is not checked, so devices are ready to respond not only to requests from their neighbors, but also to those requests that were sent from outside the network. A firewall can and should protect against such requests. But firstly, the network owners do not always install it, and secondly, port 1900 often remains open in the installed firewall. And since the response to an SSDP request can be several times, or even tens of times longer than the request itself, an amplification attack becomes possible: a fake request that arrived from the external network and contains an IP address as a reverse address of the victim host, can trigger a multiplier response and send it to the victim. And then, as in the classic DDoS scenario: either the communication channel of the victim node will be clogged with garbage, or the node itself

will drown, trying to process a powerful stream of SSDP responses.

To minimize SSDP attacks, you need to:
Block both inbound and outbound UDP port 1900 in the firewall for inbound traffic.
Use BGP flowspec to restrict incoming traffic from this port and to this port.
Use UDP-based services with extreme caution, as UDP-based DDoS attacks are more difficult to counter.
Regularly scan devices connected to the network for the enabled SSDP function and always disable it if it is not required now.

Terminal Questions:

1: What is FTP? How does it work?
2: What is NTP? Why is it important?
3: What is SSDP? What is its purpose?
4: How does FTP ensure data integrity during file transfers?
5. What security measures are available for FTP, NTP, and SSDP?

SAQ's-Self Assessment Questions
1. FTP stands for:
   a) File Transmission Protocol
   b) File Transfer Policy
   c) File Transfer Protocol
   d) File Transport Protocol
   Answer: c) File Transfer Protocol
2. NTP is used for:
   a) File transfers
   b) Time synchronization
   c) Network discovery
   d) Secure communication
   Answer: b) Time synchronization
3. SSDP is primarily used for:
   a) File transfers
   b) Network security
   c) Service discovery
   d) Time synchronization
   Answer: c) Service discovery
4. Which protocol does FTP use for communication?
   a) TCP/IP
   b) UDP
   c) HTTP