2.1 Quality of Service Definition:

Quality of Service (QoS) refers to the ability of a network to provide selected traffic with better service. This section provides an introduction to QoS in the Internet domain. The need for QoS is firstly motivated and then some mechanisms for QoS provisioning are mentioned.

2.2 The Need for Quality of Service:

From Figure 1.1 it can be seen that the number of Internet users has increased and become in hundreds of millions around the globe. With the increasing number of Internet users, more resources are required to satisfy user requirements. Commercial ventures also take advantage of the increasing number of users to create new sources of income by creating novel applications that might interest Internet users. The users and their application requirements drive the advance of the network technology.

Theoretically there are two likely drivers for network services with guaranteed QoS. One comes from applications that have strict QoS requirements such As Video-on-Demand (VoD) over the Internet and Internet Protocol (IP) telephony.

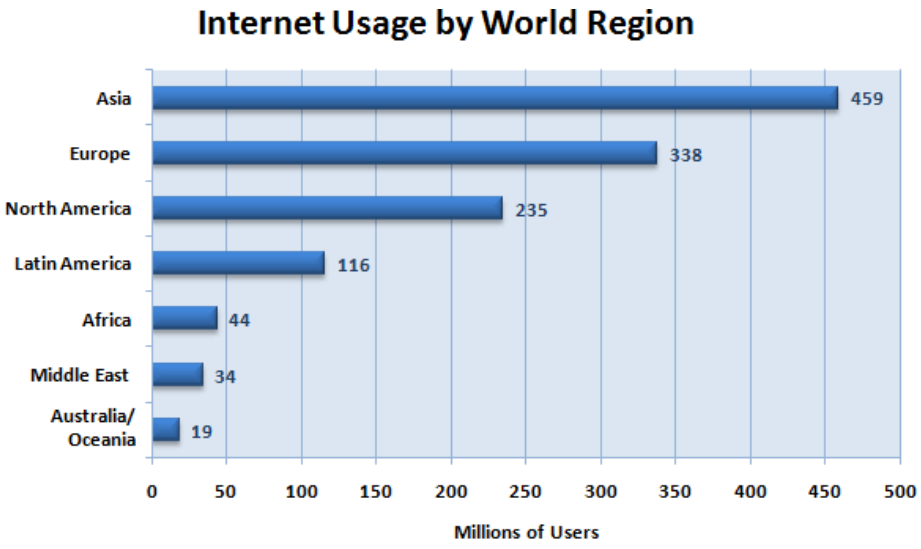

Figure .خطأ! لا يوجد نص من النمط المعين في المستند-1*Internet usage by world regions*

The second driver is the need for service differentiation. Due to the

competitive nature of the Internet marketplace network service providers will try to offer their users better quality of service guarantees than their competitors.

The network protocol used predominantly in the Internet is IP. One of the reasons for the success of IP is the fact that it is relatively simple. The design principle for IP was derived from the "end-to-end argument. This argument states that intelligent functions are limited to the edges of the network and the core is relatively unintelligent.

IP routers in the core of the network check the address of the IP datagram against a forwarding table to determine the correct next-hop interface for the datagram. If the queue for the next-hop is large, the datagram might experience delay. If the queue is full or unavailable, the router might discard the datagram. The result of this behavior is a so called "best-effort" service with unpredictable delays and data loss. [7]

Support for different types of service was one of the original design priorities of the Internet protocols. For a network service provider to be able to provide good quality of service, it should be able to provide some guarantees to the subscribers for their service. QoS is the ability of a network element to have some level of assurance that its traffic and service requirements can be satisfied. QoS does not create bandwidth rather it manages the available bandwidth according to the needs of the applications.

By providing different levels of service, one creates an incentive to steal. One user might pay for a better service and another could try to steal some of that service. As a consequence, QoS requires policy enforcement and policy management.

QoS also implies the need for accounting and billing. All these together, policy management, authentication, accounting and billing are essential to the success of QoS provision.

2.3 Providing Network QoS:

A network with quality of service has the ability to deliver data traffic with a minimum amount of delay in an environment in which many users share the same network. QoS is totally different than CoS (class of service). CoS classifies traffic into categories such as high, medium, and low (gold, silver, and bronze). Low-priority traffic is "drop eligible," while high-priority traffic gets the best service. However, if the network does not have enough bandwidth, even high-priority traffic may not get through. Traffic engineering, which enables QoS, is about making sure that the network can deliver the expected traffic loads.[8]

A package-delivery service provides an analogy. You can request priority delivery for a package. The delivery service has different levels of priority (next day, two-day and so on). However, prioritization does not guarantee the package will get there on time. It may only mean that the delivery service handles that package before handling others. To provide guaranteed delivery, various procedures, schedules, and delivery mechanisms must be in place. For example, express companies have their own fleet of planes and trucks, as well as a computerized package tracking system. Traffic engineers work out flight plans and schedule delivery trucks to make sure that packages are delivered as promised.

The highest quality of service is on a non shared communication link such as a cable that directly connects two computers. No other users contend for access to the network. A switched Ethernet network in which one computer is attached to each switch port can deliver a high level of QoS. The only contention for the cable is between the computers that are exchanging data with one another. If the link is full duplex, there is no contention.

2.4QoS Degradation Reasons:

a. Shared network links, in which two or more users or devices must contend for the same communication channel.

b. Delays caused by networking equipment (e.g., inability to process large loads).

c. Delays caused by distance (satellite links) or excessive hops (cross-country or global routed networks).

d. Network congestion, caused by overflowing queues and retransmission of dropped packets.

e. Poorly managed network capacity or insufficient capacity. If a link has fixed bandwidth, the only option to improve performance is to manage QoS.

The starting point for providing QoS in any network is to control and avoid congestion control mechanisms. What can be done to improve QoS? The obvious solution is to overprovision network capacity and upgrade to the most efficient networking equipment. This is often a practical solution in the private network environment, but not for private WAN links. Another solution is to classify traffic into various priorities and place the highest priority traffic in queues that get better service. This is how bandwidth is divided up in packet-switched networks. Higher-level queues get to send more packets, and so get a higher percentage of the bandwidth. New optical networks in the Internet coreprovide QoS with excess bandwidth. A single fiber strand can support hundreds or even thousands of wavelength circuits (lambdas). Lambdas can provide single-hop optical pathways between two points with gigabit bandwidth. A single circuit can be dedicated to traffic that needs a specific service level.

Service providers have been reluctant to implement QoS across their networks because of the management and logistics problems. If subscribers don't classify traffic in advance, then the provider will need edge devices that can classify traffic going into their networks. QoS features must also be set up from one end of a network to another, and that is often difficult to accomplish. QoS levels must be negotiated with every switch and router along a path. Still, QoS is getting easier to manage, and, in some cases, it is the only way to optimize network bandwidth.

Leading-edge service providers now offer a range of QoS service levels for Internet traffic. Subscribers specify QoS requirements in SLAs (service-level agreements).

2.5 Service-Level Agreements (SLA) Specifications forQoS:

a. **Throughput:** An SLA can specify a guaranteed data transfer rate. This is easy on virtual circuit networks such as ATM. It is more difficult on IP networks.
b. **Packet loss:**When a shared network gets busy, queues in routers and other network devices can fill and start dropping packets. A vendor may guarantee a minimum packet loss.
c. **Latency**: This is the delay in the time it takes a packet to cross a network. Packets may be held up in queues, on slow links, or because of congestion. The more networking devices a packet crosses, the bigger the delay. Delays of over 100 ms are disruptive to voice.
d. **Jitter**: Delay that is variable and difficult to interpret.

Of course, the range, location, and ownership of the network will make a big difference in how QoS is applied. An enterprise may wish to install QoS on its own intranet to support voice and video. QoS may also be applied to the LAN/WAN gateway to ensure that private WAN links or virtual private networks (VPNs) are appropriately loaded and provide quality service for inter company voice calls, videoconferences, and so on. Most of the focus for QoStechnologies on the Internet because it lacks features that can provide QoS .

2.6 Quality of Serves Techniques:

The following sections describe the various techniques that may be used to provide QoS on the Internet and in enterprise networks. Some of these solutions provide only partial QoS, but are required to provide higher levels of service. The various solutions may be categorized as follows:

a. **Congestion management:**Schemes that help reduce congestion when it occurs or that actively work to prevent congestion from occurring.
b. **Classification and queuing techniques:** Traffic is classify
c. ed according to service levels. Queues exist for each service level, and the highest priority queues are serviced first.
d. **Bandwidth reservation techniques**: Bandwidth is reserved in the network to ensure packets delivery.

e. **Packet tagging and label:** switching Packets are tagged with identifiers that specify a delivery path across a network of switches. The paths can be engineered to provide QoS.

2.7 Congestion Management Techniques:

Managing network congestion is a critical part of any QoS scheme. TCP has some rudimentary congestion controls. The technique relies on dropped packets. When a packet is dropped, the receiver fails to acknowledge receipt to the sender. The sender assumes that the receiver or the network must be congested and scales back its transmission rates. This reduces the congestion problem temporarily. The sender will eventually start to scale up its transmissions and the process may repeat.

Packets are dropped because a router queue is full or because a network device is using a congestion avoidance scheme, such as (random early detection)RED. RED monitors queues to determine when they are getting full enough that they might overflow. It then drops packets in advance to signal senders that they should slow down. Fewer packets are dropped in this scheme.[9]

The problem with RED is that it relies on dropping packets to signal congestion. ECN (explicit congestion control) is an end-to-end congestion avoidance mechanism in which a router that is experiencing congestion sets a notification bit in a packet and forwards the packet to the destination. The destination node then sends a "slow down" message back to the sender.

Traffic shaping is a technique that "smoothes out" the flow of packets coming from upstream sources so that downstream nodes are not overwhelmed by bursts of traffic. An upstream node may be a host, or it may be a network device that has a higher data rate than the downstream network. At the same time, some hosts with priority requirements may be allowed to burst traffic under certain conditions, such as when the network is not busy. A traffic shaper is basically a regulated queue that takes uneven and/or burst flows of packets and outputs them in a steady predictable stream so that the network is not overwhelmed with traffic.

2.8 Classification, Admission, and Tagging

Any QoS scheme involves guaranteeing service levels to traffic flows. In a world of infinite bandwidth, all flows could be handled equally. But networks are still bandwidth limited and congestion problems occur due to improper network design. Therefore, traffic must be classified-and, in some cases, tagged-so that downstream devices know what to do with it. Basic classification techniques are outlined here:

a. Inspect and classify (differentiate) incoming traffic using various techniques, such as "sniffing" the MAC address, the physical port on which the packet arrived, IEEE 802.1Q VLAN information, IEEE 802.1D-1998 (formerly IEEE 802.1p) information, source and destination IP address, well-known TCP/UDP port numbers, application information at layer 7, such as cookies and other information. Note that some encryption and tunneling schemes make packet sniffing impossible. Some applications never use the same port, and a variety of different applications go to port 80-the Web services port, which makes differentiating on port number difficult.

b. If a flow is requesting a particular service, use admission controls to either accept or reject the flow. Admission controls help enforce administrative policies, as well as provide accounting and administrative reporting.

c. Schedule the packets into appropriate queues and manage the queues in a way that ensures that each queue gets an appropriate level of service for its class.

Classification requires administrative decisions about how traffic should be classified and where it should be tagged. Administrators might classify traffic based on whether it is best effort and suitable for discard, real-time voice and video, network controls (e.g., OSPF messages), or mission critical. The following classification schemes identify traffic near its source and mark packets before they enter the network. Network nodes only need to read the markings and forward packets appropriately.

a. **IEEE frame tagging** This scheme defines a tag, inserted into an Ethernet frame, which contains three bits that can be used to identify class of service.
b. **IETF Differentiated Services (Diffserv):** Diffserv is an IETF specification that works at the network layer. It alters bits in the IP ToS field to signal a particular class of service. Diffserv works across networks, including carrier and service provider networks that support the service; and, therefore, it has become an important scheme for specifying QoS across the Internet. Diffserv is covered in more details in this dissertation.

The first scheme works over LANs, while Diffserv works over internetworks. The tag information in MAC-layer frames will be lost if the frame crosses a router. However, some method may be used to capture the information and use it to set Diffserv markings.

2.9 MAC-Layer Prioritization

As mentioned, the IEEE defined a method for inserting a tag into an IEEE MAC-layer frame that contains bits to define class of service. During development, this was known as Project 802.1p, and you will see it referred to that way in much of the literature. It is now officially part of IEEE 802.1D-1998. The tag defines the following eight "user priority" levels that provide signals to network devices as to the class of service that the frame should receive:

a. Priority 7,6: Network control traffic such as router configuration messages
b. Priority 5 : Voice traffic, such as NetMeeting, that is especially sensitive to jitter
c. Priority4 : Video, which is high bandwidth and sensitive to jitter
d. Priority 3 : Better than best effort, which would include important business traffic that can tolerate some delay
e. Priority 2 : Best-effort traffic
f. Priority 1 : The default mode if none is specified
g. Priority 0: Non critical traffic such as backups, non critical replications, some electronic mail, and so on

A method for reordering and moving delay-sensitive real-time traffic to the front of a queue is also defined. A component of this scheme is GARP (Group Address Registration Protocol), which is used by LAN switches and network-attached devices to exchange information about current VLAN configurations. Note that 802.1D-1998 provides at the LAN level what Diff-Serv provides in layer 3 across internetworks. MAC-layer tags may be used to signal a class of service to Diffserv.

2.10 IP Type of Service (IP ToS):-

The role of the IP ToS field has changed with the development of Diff-Serv. The original meaning of the ToS field was defined in RFC791 (Internet Protocol, September 1981); however, it was never used in a consistent way. Most routers are aware of the field, but it has little meaning across public networks. Many enterprises have used it internally to designate various classes of service or to prioritize traffic across private WAN links.
The ToS field is divided into two sections: the Precedence field (three bits) and a field that is customarily called "Type-of-Service" or "TOS" (five bits). Diffserv redefined the field as the Diffserv Field (DS Field). RFC 2474 (Definition of the Differentiated Services Field in the IPv4 and IPv6 Headers, December 1998) describes this further.

2.11 IETF QoS Solutions:-

The IETF has been working to define Internet QoS models for many years. The task has not been easy since packets must cross many networks, and providers must agree not only how QoS will be managed, but also how it is paid for. The primary QoS techniques developed by the IETF are Intserv (Integrated Services), Diffserv (Differentiated Services), and MPLS (Multiprotocol Label Switching), as described next.

a. **Best Effort:**Best-effort delivery is the default method—traffic is sent out in the order it arrives with no differentiation between types of traffic and no guarantee of delivery. Benefits of best effort include its scalability (the Internet is based on best-effort delivery), and its ease of deployment. Drawbacks include the fact that all traffic is given the same service level.
b. **Integrated Services (Intserv):** This is a model for providing QoS on the Internet and intranets. The intention of Intserv designers was to

set aside some portion of network bandwidth for traffic such as real-time voice and video that required low delay, low jitter (variable delay), and guaranteed bandwidth. The Intserv Working Group developed RSVP (Resource Reservation Protocol), a signaling mechanism to specify QoS requirements across a network. Intserv has scalability problems and it was too difficult to deploy on the Internet. However, RSVP is used in enterprise networks, and its control mechanism for setting up bandwidth across a network is being used in new ways with MPLS.

c. **Differentiated Services (Diffserv):** Diffserv classifies and marks packets so that they receive specific per-hop forwarding at network devices along a route. The important part is that Diffserv does the work at the edge so that network devices only need to get involved in properly queuing and forwarding packets. Diffserv works at the IP level to provide QoS based on IP ToS settings. Diffserv is perhaps the best choice for signaling QoS levels available today and it is going to be discussed in details in this dissertation.

2.12 Policies and Policy Protocols:-

The final pieces of the QoS picture are policies, policy services, and policy signaling protocols. Most of the QoS systems just described use policy systems to keep track of how network users and network devices can access network resources. A defining feature of a policy system is that it works across a large network and provides policy information to appropriate devices with that network. [9].

Policy architecture consists of the following components, which primarily manage the rules that govern how network resources may be used by specific users, applications, or systems. When rules are specified and programmed into policy systems, they are known as policies.

a. **Policy** clients Network devices that process network traffic such as switches and routers running various queuing algorithms. Policy clients query policy servers to obtain rules about how traffic should be handled.

b. **Policy servers** This is the central authority that interprets network policies and distributes them to policy clients.

c. **Policy information system** The information about whom or what can use network resources is stored in some type of database, usually a directory services database.

This architecture allows network administrators to specify policies for individuals, applications, and systems in a single place-the policy information system. The policy server then uses protocols such as LDAP (Lightweight Directory Access Protocol) or Structure Query Language (SQL) to obtain this information and form policies that can be distributed to policy clients. Policy clients talk to policy servers via network protocols such as COPS (Common Open Policy Service) and SNMP (Simple Network Management Protocol). COPS are an intra domain mechanism for allocating bandwidth resources and it is being adapted for use in establishing policy associated with a Diffserv capable networks.