IntServ implementation has four important components: the signaling protocol (RSVP), the admission control routine, the classifier and the packet scheduler. After the resource reservation and call admission processes are complete, when a router receives a packet, the classifier performs a classification and inserts the packet in a specific queue based on the classification result. The packet scheduler will then schedule the packet accordingly to meet its QoS requirements.

Fig. 11 shows, how these components might fit into an IP router that has been extended to provide integrated services. The router has two broad functional divisions: the forwarding path below the double horizontal line, and the background code above the line. The forwarding path of the router is executed for every packet and must therefore be highly optimized. Indeed, in most commercial routers, it is implemented in hardware.

The forwarding path is divided into three sections: input driver, Internet forwarder, and output driver. The Internet forwarder interprets the IP header. For each packet, an Internet forwarder executes a suite-dependent classifier and then passes the packet and its class to the appropriate output driver. A classifier must be both general and efficient. For efficiency, a common mechanism should be used for both resource classification and route lookup. The output driver implements the packet scheduler.

The background code is simply loaded into router memory and executed by a general-purpose CPU. These background routines create data structures that control the forwarding path. The routing agent implements a particular routing protocol and builds a routing database. The reservation setup agent implements the protocol used to set up resource reservations. If admission control gives the "OK" for a new request, appropriate changes are made to the classifier and packet scheduler database to implement the desired QoS. Finally, every router supports an agent for network management. This agent must be able to modify the classifier and packet scheduler databases to set up controlled link sharing and to set admission control policies. The implementation framework for a host is generally similar to that for a router, with the addition of applications. Rather than being forwarded, host data originates and terminates in an application. An application needing a real-time QoS for a flow must somehow invoke a local reservation setup agent.

As stated earlier IntServ has been designed to provide two types of services:

- Guaranteed Service for applications requiring fixed delay bound
- Predictive Service for applications requiring probabilistic delay bound. The implementations of the guaranteed service and the predictive service are defined in the guaranteed service RFC [13] and the controlled load service RFC [23], respectively.

The IntServ architecture represents a fundamental change to the Internet architecture but it is beset with many problems, which makes it very difficult to deploy. Some of the important problems are the following:

- The amount of state information increases proportionally with the number of flows. This places a huge storage and processing overhead on the routers. Therefore, this architecture does not scale well in the Internet core;
- The requirement on routers is high. All routers must implement RSVP, admission control, MF classification and packet scheduling;
- Ubiquitous deployment is required for guaranteed service. Incremental deployment of Controlled-Load Service is possible by deploying Controlled-Load Service and RSVP functionality at the bottleneck nodes of a domain and tunneling the RSVP messages over other part of the domain.

14.2 Differentiated Services

To overcome the limitations of IntServ, IETF proposed Differentiated Services (DiffServ) [15], which is simpler and more scalable. DiffServ redefines the IPv4 Type of Service (TOS) field or IPv6 Traffic Class Byte as differentiated service (DS) field. The first six bits of the field are called as DS Code point, which when marked differently indicates the behavior (known as per-hop behavior or PHB) each router is required to apply to individual packets.

The information required by the buffer management and scheduling mechanisms is carried within the packet. Therefore, differentiated services do not require special signaling protocols to control the mechanisms that are used to select different treatment for the individual packets. Consequently, the amount of state information, which is required to be maintained per node, is proportional to the number of service classes and not proportional to the number of application flows, which is major improvement over IntServ.

A customer must have service level agreement (SLA) with its ISP in order to receive DiffServ. An SLA specifies the class of service supported and the amount of traffic allowed in each class. An SLA can be static or dynamic. Static SLAs are negotiated on a regular, e.g. monthly and yearly, basis. Customers with Dynamic SLAs must use a signaling protocol, e.g. RSVP, to request for services on demand.

14.3 Functional Elements of DiffServ Architecture

The Differentiated Services architecture [46] is composed of a number of functional elements, namely packet classifiers, traffic conditioners and per-hop forwarding behaviors (PHB). These are described below:

Packet Classifiers: Packet classification is normally done at the edge of the DS domain by packet classifiers, which select packets based on the content of packet headers. Two types of classifiers are currently defined: the Behavior Aggregate (BA) classifier, which selects packets based on the DS CodePoint only, and the Multi-Field (MF) classifier, which performs the selection based on the combination of one or more header fields, such as source address, destination address, type-of service byte, protocols ID, source port number and destination port number.
Traffic Conditioners: Traffic conditioners form the most vital part of a differentiated services network. Their goal is to apply conditioning functions on the previously classified packets according to a predefined Traffic Class Specification in SLA. A traffic conditioner consists of one or more of the following components:

Meter: A device which measures the temporal properties of a traffic stream selected by a classifier.
Marker: A device that sets the DS CodePoint in a packet based on well-defined rules.
Shaper: A device that delays packets within a traffic stream to cause the stream to conform to some defined traffic profile (See Sec- 3.6).
Dropper/Policer: A device that discards packets based on specified rules (See Sec. 3.6).

Per-Hop Behavior (PHB): A PHB is a description of the externally observable forwarding behavior of a differentiated services node, applied to a collection of packets with the same DS CodePoint that are crossing a link in a particular direction (called differentiated services behavior aggregate). Each service class is associated with a PHB. PHBs are defined in terms of behavior characteristics relevant to service provisioning policies, and not in terms of particular implementations. PHBs may also be specified in terms of their resource priority relative to other PHBs, or in terms of their relative observable traffic characteristics. Currently there are three proposed PHBs that are briefly described below.

- The Default (DE) PHB is the common, best-effort forwarding available in today's Internet. IP packets marked for this service are sent into a network without adhering to any particular rules and the network will deliver as many of these packets as possible and as soon as possible but without any guarantees.
- Assured Forwarding (AF) PHB is a means for a provider differentiated services domain to offer different levels of forwarding assurances for IP packets received from a customer differentiated services domain.