Differentiated Services

Anjali Agarwal

Disadvantages of Integrated Services

◆ Routers keep flow-specific state for each flow

◆ State information increases with number of flows

◆ Routers need large storage space and high processing power

◆ Routers more complex – need to implement RSVP protocol, admission control, packet classifier, per-flow packet-scheduling algorithm

Assignment Project Exam Help

https://powcoder.com

Add WeChat powcoder

Differentiated Services

♦ Differentiated Services (DiffServ) model is designed to be scalable and to provide QoS

♦ Traffic is aggregated into a limited number of classes

♦ Service is on aggregated flow basis, not per individual flow – more scalable

♦ Each class receives a well-defined service treatment at each DiffServ router

♦ No per-flow signaling

♦ Differentiated services are intended to provide scalable service discrimination in the Internet without the need for per-flow state and signaling at every hop, by

  » *setting bits in the TOS octet, only at network edges, to specify a particular forwarding treatment that a packet receives at a given network node*

  » *using those bits to determine how packets are treated by the routers inside the network, (per-hop behaviors probably need to be available in all routers in a differentiated-services-capable network) and*

  » *traffic conditioning (classification, marking, policing and shaping) only at network boundaries in accordance with the requirements of each service – although DS byte classifier required in all network nodes*

- Differentiated Services avoids simple priority tagging and depends on more complex policy or rule statements to determine how to forward a given network packet.

- An analogy is made to travel services, in which a person can choose among different modes of travel - train, bus, airplane - degree of comfort, the number of stops on the route, standby status, the time of day or period of year for the trip, and so forth.

- For a given set of packet travel rules, a packet is given one of 64 possible forwarding behaviors - known as per hop behaviors (PHBs). A six-bit field, known as the Differentiated Services Code Point (DSCP), in the Internet Protocol (Internet Protocol) header specifies the per hop behavior for a given flow of packets.

- behavior aggregate: a collection of packets with the same DS byte pattern crossing a boundary in a particular direction.

The DS Field layout
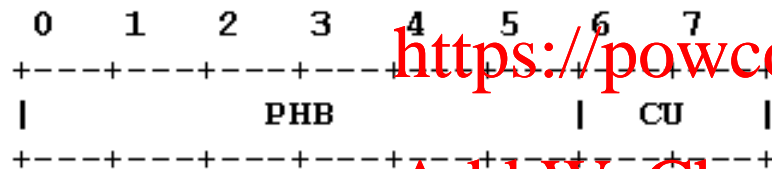
```
   0   1   2   3   4   5   6   7
 +---+---+---+---+---+---+---+---+
 |          PHB          |   CU  |
 +---+---+---+---+---+---+---+---+

 PHB: per-hop behavior
 CU:  currently unused

(bit 0 = most significant if relevant)
```
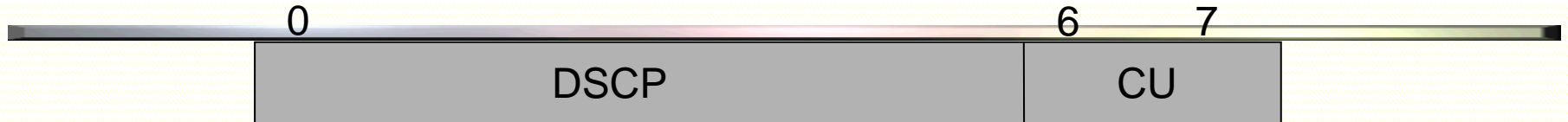
The structure of the DS byte shown is incompatible with the existing definition of the IPv4 TOS octet

To maintain compatibility with IPv4 hosts and networks which utilize the existing TOS semantics, a differentiated services-enabled network **must** remark the TOS value of packets arriving at a boundary entry node to some acceptable value within the new semantics

♦ **Bit 0 - "In Profile" bit**
♦ **Bits 1 to 5 – PHB bits**

6

Differentiated Services Field

```
0                                    6   7
┌──────────────────────────────┬─────────┐
│            DSCP              │   CU    │
└──────────────────────────────┴─────────┘
```

"Currently Unused"

♦ Differentiated Services Code-point (DSCP)

» *Six bits in the IPv4 TOS field*

» *DSCP value specifies PHB in core router*

» *Router uses DSCP as index into per-class buffering & scheduling treatment for a packet*

» *A recommended set of DSCP-to-PHB mappings*

– But service providers free to choose their own mapping

» *TOS Backwards Compatibility:*

– 000000→Default (Best Effort), 11x000→Network Control

7

♦ DS byte selects which treatment a particular packet receives –

> » *an ISP may configure eight weighted round robin queues in its routers and use the DS byte to select which queue*

> » *an ISP might configure a single queue with multiple drop priorities and use the DS byte to select the drop preference (from zero, most likely to drop to seven, least likely to drop)*

> » *an ISP may configure four queues with two levels of drop preference in each*

♦ It is undesirable for the "same" per-hop behavior to be selected by different DS byte values in different ISPs.

Widely used Per-Hop Behaviours

♦ Default (DE) –

   » *the common, best-effort forwarding available in today's internet*

   » *Delay requirements are as soon as possible, and the corresponding bandwidth requirements are as much as possible*

   » *PHB field value: 00000*

♦ Expedited Forwarding (EF) –

   » *may be used to implement services requiring low delay and low jitter, and may also be useful for network control traffic*

   » *EF-marked packet always gets the next opportunity to send a packet*

   » *PHB field value: 11100*

Per-Hop Behaviors

♦ Several PHBs defined by IETF

♦ DE (Default) PHB: Best effort

♦ Expedited Forwarding (EF) PHB: "Premium"

  » *Low loss, low latency, low jitter, assured-bandwidth end-to-end transfer*

♦ Assured Forwarding (AF) PHB: "Better than Best Effort"

  » *High assurance of delivery if traffic profile kept*

  » *Four independent AF classes*

    – Provide four levels of assurance

    – Three values of packet drop precedence within each level

    – Router must preserve sequence of packets within same microflow (same application flow, same AF level)

PHB and Traffic Management

- ♦ PHB definition do not specify mechanism to implement behavior
- ♦ EF PHB
  - » *HOL priority queueing, Weighted Fair Queueing, or combination*
- ♦ AF PHB: Different levels of drop-precedence

Assignment Project Exam Help

https://powcoder.com

Add WeChat powcoder

♦ "In Profile" bit

    » *IN bit set - experiences a probability of loss or congestion indication which is always less than or equal to that experienced by packets with IN bit is cleared*

    » *IN bit should be set to zero for Default traffic*

    » *All packets marked EF should have the IN bit set*

The value of the DS byte may be modified at each network boundary (possibly subject to some negotiated policy).

The value of the DS byte does not have end-to-end integrity;

Security and transport protocol checksums MUST not include this field.

Forwarding Path Architecture

Complexity at the Edge

TCA
…

SLA

Notwithstanding …

Assignment Project Exam Help

https://powcoder.com

Add WeChat powcoder

DiffServ Domain

H

H

A

A

C

A

C

C

A

H

A

A

H

C = Core Router

A = Access Router

H = Host

♦ User negotiates *Service Level Agreement (SLA)* with service provider
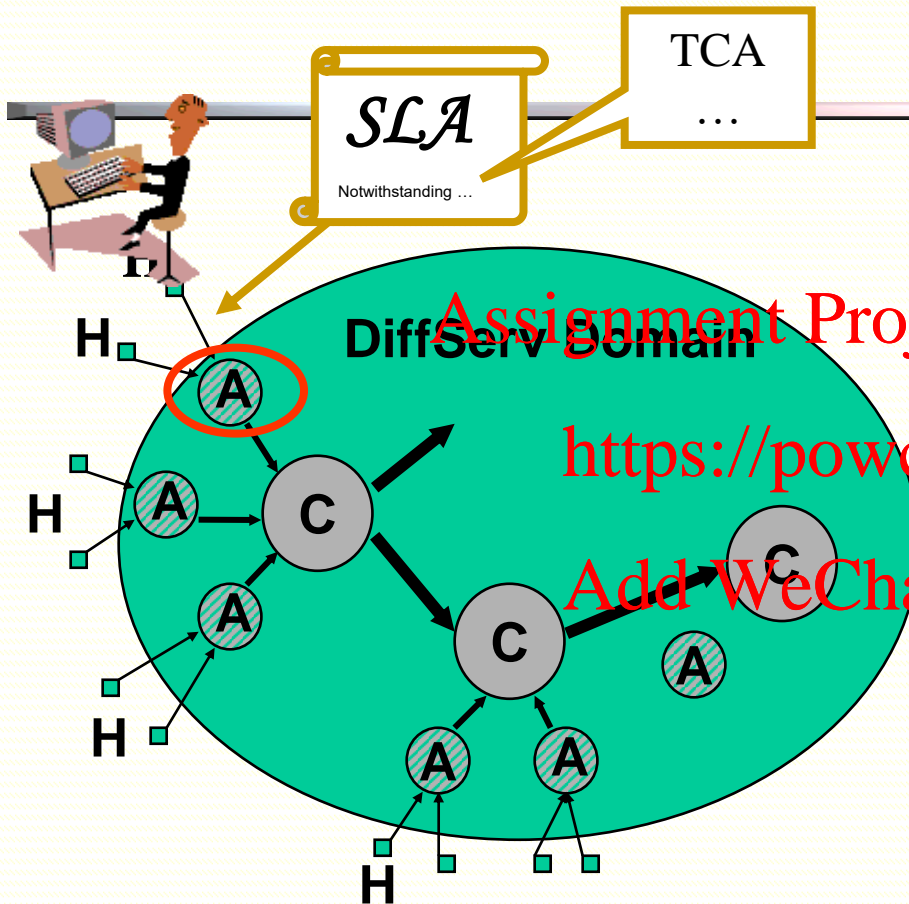
 » *Static or dynamic (needs BB)*

♦ SLA includes a *Traffic Conditioning Agreement (TCA)* stipulating

 » *service level, traffic profile, marking, shaping*

♦ *Access Router*

 » *classifies user packets and marks them in* DS *field of IP header as belonging to a specific class*

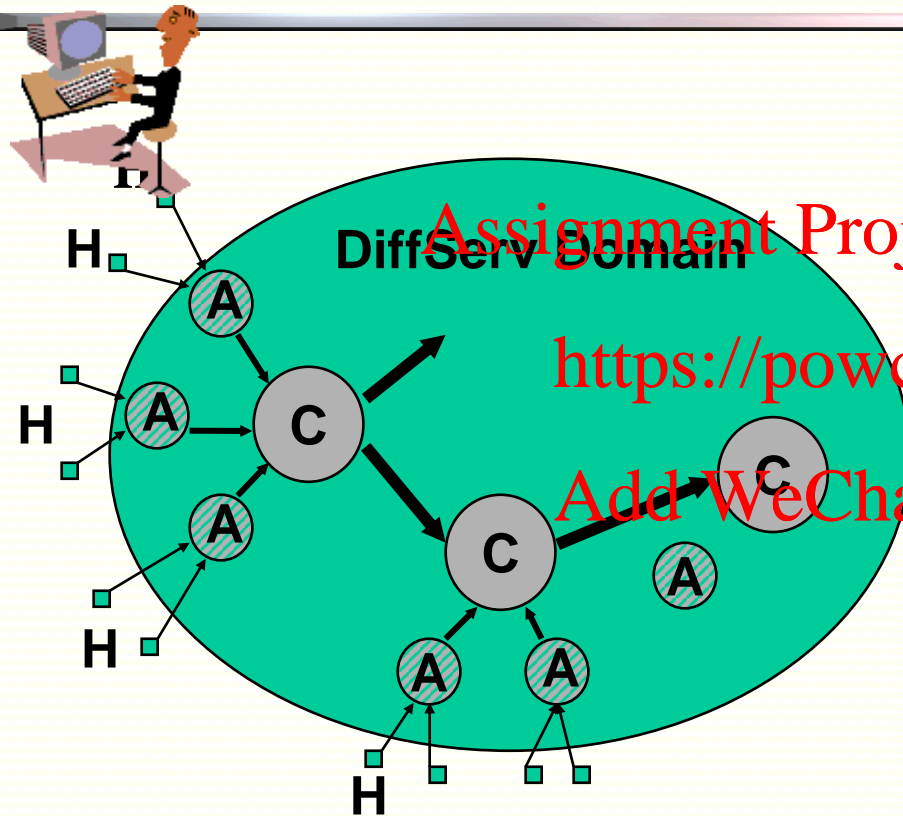 » *conditions packet stream so it conforms to profile*

Forwarding Path Architecture

Simplicity in the Core

DiffServ Domain

A
C
A
C
C
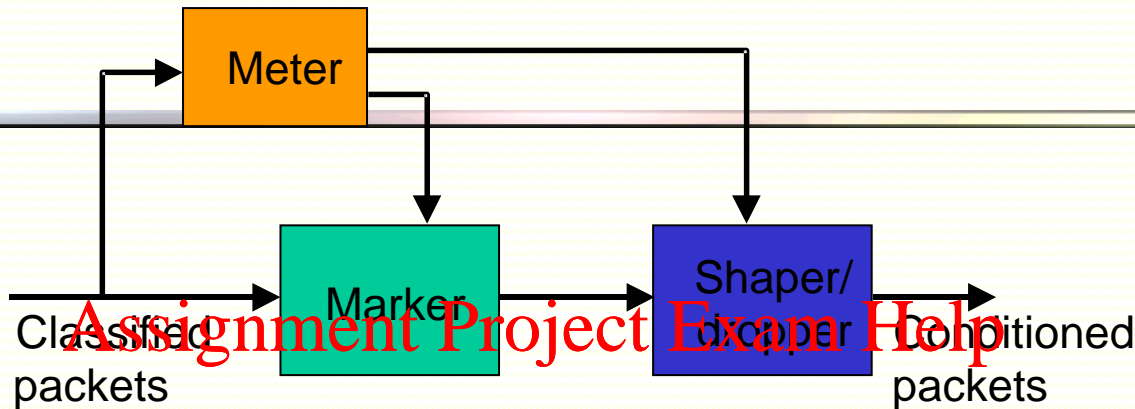**A**
A
A

H
H
H
H
H

- ◆ Aggregate-flow or class identified by a particular value in the DS field

- ◆ Core routers provide a limited number packet forwarding options called *Per-Hop Behaviors (PHBs)*

- ◆ *Value in DS field* identifies class and PHB

- ◆ Router resources reserved on aggregate-flow basis, not per-flow
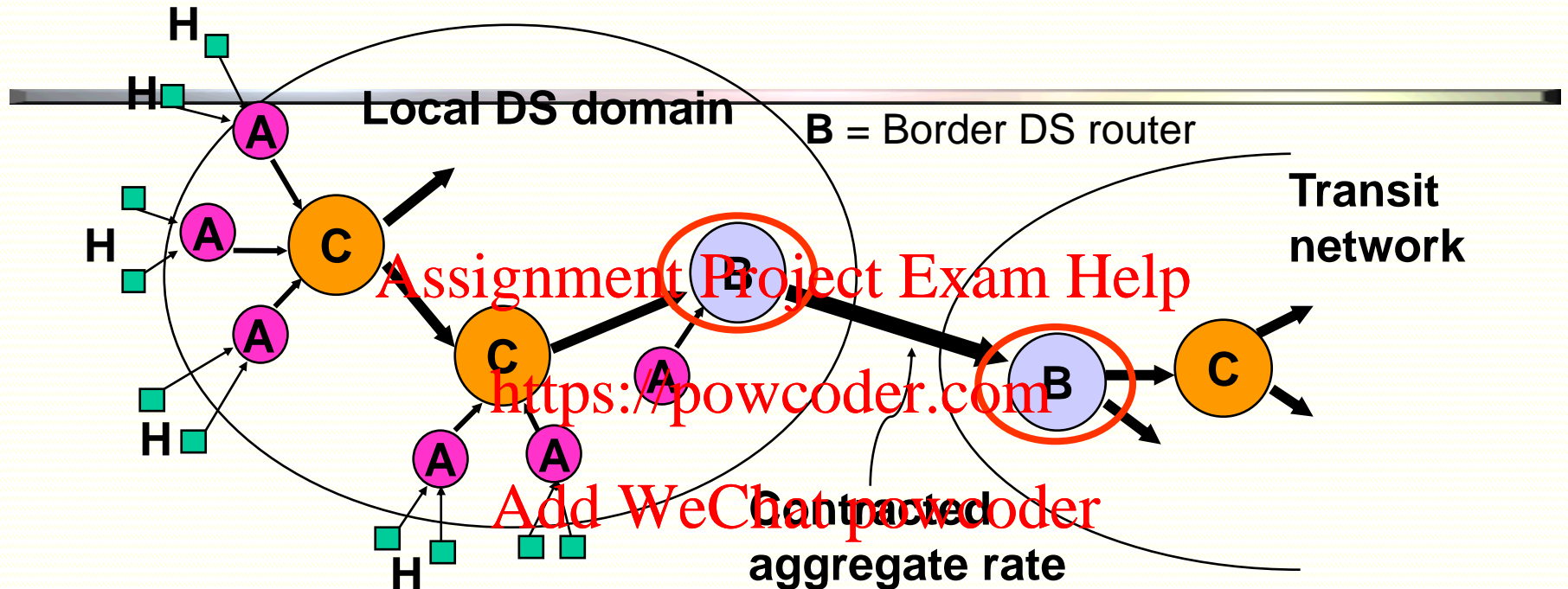
C = Core Router

A = Access Router

H = Host

14

Traffic Conditioner

Meter

Marker

Shaper/
Dropper

Classified
packets

Conditioned
packets

Assignment Project Exam Help

https://powcoder.com

Add WeChat powcoder

- ◆ *Meter* measures traffic and checks for conformance to traffic profile
  - » *Token bucket to check peak rate, sustained rate, maximum burst size*
- ◆ *Marker* sets DSCP
  - » *Remark to lower class if non-conforming*
- ◆ *Shaper/Dropper:* Shape to profile; drop non-conforming packets

DiffServ across Domains

H

H

Local DS domain

B = Border DS router

H

A

A

C

Assignment Project Exam Help

B

Transit network

https://powcoder.com

C

A

B

C

H

Add WeChat powcoder

A

A

contracted aggregate rate

H

- ◆ SLA must be in place between domains
- ◆ Egress border router must condition traffic to contracted profile

- ◆ Ingress border router classifies & conditions traffic
- ◆ DSCP values may need to be mapped if domains use different DSCP-PHB mappings

16

Bandwidth Broker

♦ *Bandwidth Broker* responsible for allocating and controlling bandwidth within a DS domain

♦ Users contact BB to negotiate SLA

» *BB uses policy database to determine whether a user can request certain services*

» *BB determines whether resources are available to handle a request*

» *BB translates flow database into TCAs to setup packet classifiers & meters in edge routers*

♦ BB allocates traffic to classes within domain

♦ BB negotiates agreements with other DS domains

Features

♦ Differentiated services does not require end-to-end signaling, but permits each domain to develop allocations of its intra-domain traffic according to rules and processes that are as simple or complex as desired

♦ Differentiated services are realized by the concatenation of per-hop behaviors along the transport packet; therefore, the treatment experienced by a behavior aggregate along a particular path is unpredictable if some of the nodes along that path do not recognize and implement the proposed per-hop behaviors

A Framework for End-to-End QoS Combining RSVP/Intserv and Differentiated Services
http://diffserv.lcs.mit.edu/Drafts/draft-bernet-intdiff-00.txt

♦ intserv and diff-serv are complementary tools in the pursuit of end-to-end QoS

♦ Deployment of diff-serv capable core networks and intserv capable stub networks at the periphery

♦ admission control is provided implicitly by Diff-serv, by policing at ingress points. The problem with implicit admission control is that it breaks the end-to-end validity of explicit admission control. RSVP capable intserv nodes should be explicitly informed of admission control failure in the diff-serv network

♦ Host –

  » *Both sending and receiving hosts use RSVP to communicate QoS requirements*

  » *may mark the DS-byte in transmitted packets, or Leaf routers within the intserv network may do that on their behalf.*

♦ Edge Routers –

  » *consist of two halves, the standard RSVP half, which interfaces to the stub networks, and the diff-serv half, which interfaces to the transit network.*

♦ Boundary Routers –

  » *are not required to run RSVP but are expected to implement the policing function of diff-serv ingress routers*

  » *are not required to mark the DS-byte*

The boundary between the RSVP/Intserv network and the diff-serv network is placed within the edge routers at the stub networks, but may be shifted to the transit network.

- ◆ Stub Networks –
  - » *consist of RSVP capable hosts and some number of leaf routers*
  - » *Leaf routers and hosts in a non-RSVP capable leaf are assumed to be RSVP capable, if not pass RSVP messages unhindered*
- ◆ Transit Network –
  - » *not RSVP capable, but is able to carry RSVP messages transparently*
  - » *diff-serv capable - provides levels of service based on the DS-bytes*
- ◆ Mapping from Intserv Service Type to DS-Byte –
  - » *unique code points are allocated for each service in the service type field of the Intserv flowspec*

How End-to-End QoS is Obtained

1. The sending host's QoS process generates an RSVP PATH message, describing the traffic offered by the sending application.

2. The PATH message is carried toward the receiving host. In the sending stub network, standard RSVP processing will be applied at RSVP capable nodes (routers, etc).

3. At ER1, PATH state is installed in the router. The PATH message is sent onward, to the transit network.

4. The PATH message is carried transparently through the transit network. It is processed in the receiving stub network according to standard RSVP processing rules.

5. At the receiving host, the QoS process generates an RSVP RESV message, indicating interest in the offered traffic, at a certain intserv service level. The RESV message is carried back towards the sending host.

How End-to-End QoS is Obtained (cont.)

6. At ER2, the RESV message is subjected to standard RSVP processing. It may be rejected if resources on the downstream interface of ER2 are deemed insufficient to carry the resources requested. If it is not rejected, it will be carried transparently through the transit network, arriving at ER1.

7. The RESV message triggers diff-serv admission control service (DACS) processing. DACS compares the resources requested to the resources available at the corresponding diff-serv service level, in the diff-serv enabled transit network

8. Assuming the available capacity is sufficient, the RESV message is admitted and is allowed to continue upstream towards the sending host. If the available capacity is insufficient, the RESV message will be rejected.

How End-to-End QoS is Obtained (cont.)

9. The RESV message proceeds through the sending stub network. RSVP nodes in the sending stub network may reject it. If it is not rejected, it will arrive at the sending host.

10. At the sending host, the QoS process receives the RESV message. It interprets receipt of this message as an indication that the specified traffic has been admitted for the specified intserv service type (in the RSVP enabled regions of the network) and for the corresponding diff-serv service level (in the diff-serv enabled regions of the network). It begins to set the DS-byte in the headers of transmitted packets, to the value which maps to the Intserv service type specified in the admitted RESV message.

Issues

Setting the DS-Byte at Hosts - hosts may attempt to 'steal' resources

> *policing within the stub network and/or at the interface to the transit network is a straightforward architecture*

> *boundary routers need only to provide BA classification and to police to ensure that the customer is not exceeding the aggregate capacity negotiated for the service level*

Sending host does not do the marking

> *intermediate and/or boundary routers must provide MF classification (on the DS byte as well as any one of a number of header fields like a RSVP classifier), mark and police*

Diff-Serv vs Int-Serv

♦ **only a limited number of service classes indicated by the DS field.**

♦ **amount of state information is proportional to the number of classes rather than the number of flows – Diff-serv more scalable**

♦ **easier to implement and deploy Differentiated Services - sophisticated classification, marking, policing, and shaping operations are only needed at boundary of the networks. ISP core routers need only to implement *Behavior Aggregate* (BA) classification.**

Diff-Serv vs Int-Serv

♦ **Core routers must forward packets very fast and therefore must be simple. Boundary routers need not forward packets very fast because customer links are relatively slow. Therefore, they can spend more time on sophisticated classification, policing and shaping**

♦ **DS-incapable routers simply ignore the DS fields of the packets and give the Assured Service packets Best Effort Service. Overall performance of Assured Service traffic will still be better than the Best Effort traffic.**

Assignment Project Exam Help

https://powcoder.com

Add WeChat powcoder