Security in Differentiated Services Networks

Venkatesh Prabhakar
Srinivas R. Avasarala
Sonia Fahmy

{vp, sra, fahmy}@cs.purdue.edu
http://www.cs.purdue.edu/homes/fahmy/cerias

Terminology - I

- **Per-Hop-Behaviour (PHB):** The forwarding behaviour experienced by a traffic flow in a DS domain.
- **Differentiated Services Code Point (DSCP):** A specific field in the IP header used to select a PHB.
- **Service Level Agreement (SLA):** A service contract between a customer and a service-provider that specifies the forwarding service a customer would receive.

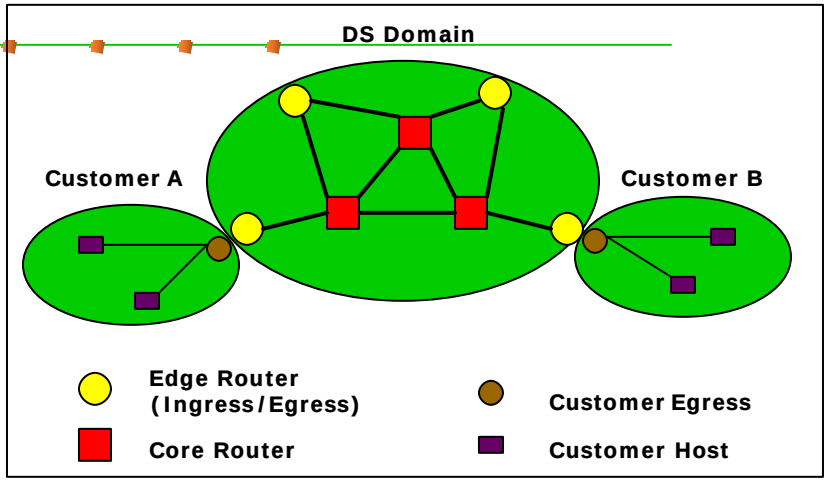
Terminology - II

- **Assured Forwarding (AF):** A PHB group that provides different levels of forwarding assurances by using different traffic classes, each with multiple drop precedences.
- **Expedited Forwarding (EF):** A PHB that provides low loss, low latency, low jitter, guaranteed bandwidth service.
- **Multi-Field (MF) Classifier:** A classifier that selects packets based on a combination of fields in the IP header.
- **Behaviour Aggregate (BA) Classifier:** A classifier that selects packets based on the DSCP field in the IP header.

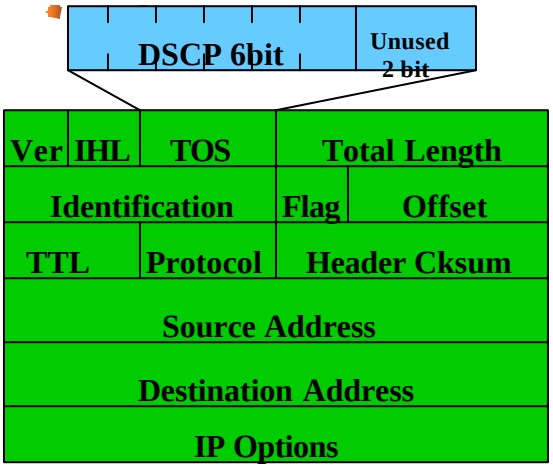
Terminology - III

- **Meter:** A device that measures the traffic rates of flows.
- **Marker:** A device that marks the DSCP field in the IP packet header with values based on SLAs.
- **Shaper:** A device that delays packets in a traffic stream to cause it to conform to a defined traffic profile.
- **Dropper:** A device that drops out-of-profile traffic from a traffic stream.

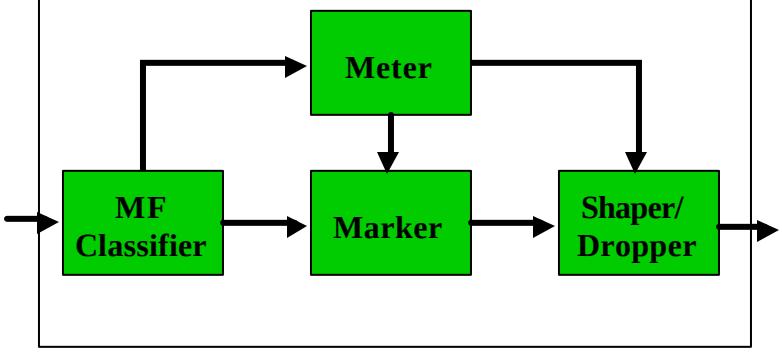
DiffServ Architecture



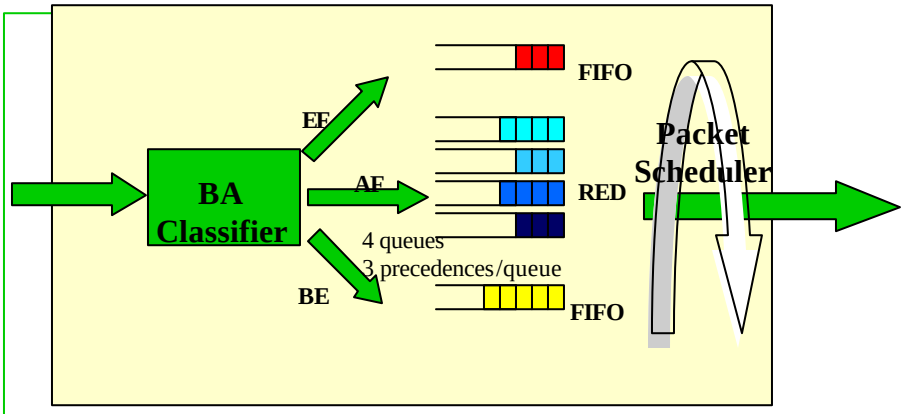
DiffServ Code Point (DSCP)



Ingress Router Functionality



Core Router Functionality



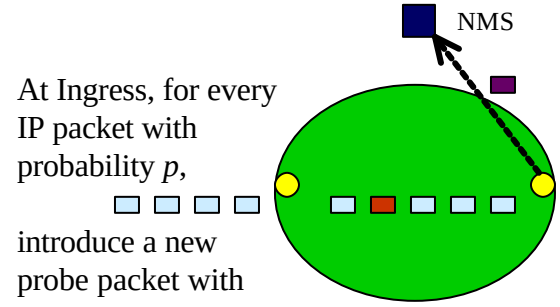
Attacks on the DS framework I

- **Network provisioning attacks:** Automatic signalling protocols like RSVP or SNMP are used to configure DS nodes from policy distribution points (bandwidth brokers). This process can be attacked by injecting bogus configuration messages, modifying real messages, delaying or dropping them.
- **Solution:** Employ encryption of configuration message exchanges of these signalling protocols.

Attacks on the DS Framework II

- **Data Forwarding process:** Traffic can be injected into the network either to steal bandwidth or cause QoS degradation by causing other customer flows to experience longer delays and higher loss rates.
- **Solution:** We need intrusion detection and response systems to protect QoS in such cases. We propose a distributed monitoring approach with measurement of traffic characteristics like delays and loss rates at all the DS nodes. A network mgmt. station (NMS) collects all the measurements and analyses them to detect violations.

Delay Measurements

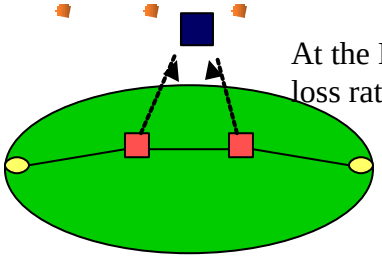


At Ingress, for every IP packet with probability *p*, introduce a new probe packet with current timestamp

At Egress, use current time – probe timestamp to measure delay and report to NMS in a control packet

Edge Router IP Packet Probe Packet Control Packet

Loss Measurements

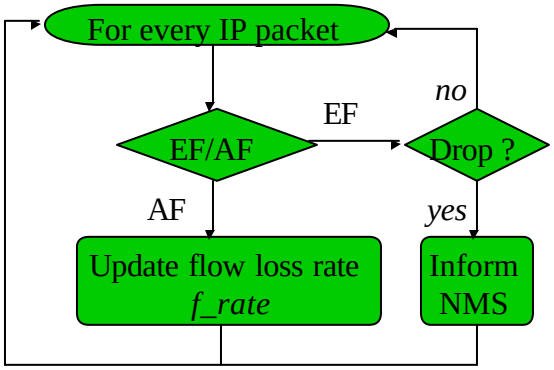


At the NMS, average the reported loss rates and compare against SLA

At the core routers, measure loss rate for all flows and classes. When loss rate of a class exceeds its threshold inform loss rate of the flow to NMS.

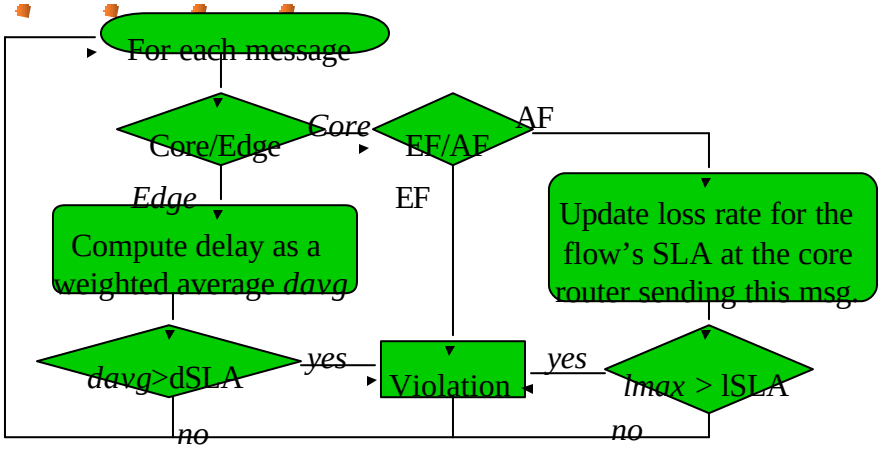
Edge Router NMS Core Router

Processing at Core Router



Periodically, with time period *t*, send the loss rates of all flows with loss rates within a fraction *k* of the flow with the highest loss rate.

Processing at NMS



Testbed Setup