Introduction to Differentiated Services (DiffServ) and HP-UX IPQoS

What is Quality of Service (QoS)? ......................................................................................................... 2
Differentiated Services (DiffServ) ............................................................................................................ 2
  Overview ........................................................................................................................................ 2
  Example – XYZ Corporation .............................................................................................................. 2
Components of DiffServ ........................................................................................................................ 3
  Traffic Classification and Conditioning ............................................................................................... 3
    Classification ............................................................................................................................... 3
    Conditioning................................................................................................................................ 4
HP-UX IPQoS ....................................................................................................................................... 6
  Configuration .................................................................................................................................. 6
    Filters.......................................................................................................................................... 6
    Policies ....................................................................................................................................... 6
    Adapters ..................................................................................................................................... 7
Summary ............................................................................................................................................ 8
For More Information ........................................................................................................................... 9
  Request for Comments ...................................................................................................................... 9
  Associated HP IP Quality of Service (IPQoS) documents ............................................................. 9
What is Quality of Service (QoS)?

Many of today’s IP networks provide what is referred to as “Best Effort Service”. Delivery of an IP packet is accomplished without differentiating between the requirements of specific traffic flows such as voice, video, or data. Voice and video, for example, require minimal interruptions in packet flow to avoid jitter and delays during communication. Data, on the other hand, may only require that it reaches its destination within a reasonable timeframe. Quality of Service (QoS) was designed to provide a mechanism to allocate different levels of service or priority based on application needs of the application or on organizational requirements. The type of mechanism used to provide these levels of service can vary from one QoS implementation to another and can include dedicated bandwidth allocation and VLAN marking.

Practical application of QoS can have a wide range of uses that can classify and condition traffic flows based on an organization’s operational goals as well as the time-critical exchange of information such as 9-1-1 emergency, communication between remote hospitals an ocean apart, Homeland Security, and National Defense.

This white paper focuses on the Differentiated Services (DiffServ) model of QoS.

Differentiated Services (DiffServ)

Overview

The Differentiated Services (DiffServ or DS) model classifies and, if needed, conditions traffic streams to conform to specified levels of service as defined by Service Level Agreements (SLAs). A DS Domain is defined by a contiguous set of nodes provisioned with the same service policies and PHB definitions. The classification and conditioning of packets occurs on DS boundary nodes (or interior nodes - with limited conditioning) within the organization’s core network and other DS Domains. The packets are marked and conditioned by the DS nodes to receive a specific level of service as they traverse the network to their final destination.

The following sections use an example scenario to illustrate DiffServ QoS concepts, classification, conditioning, and operation.

Example – XYZ Corporation

The XYZ Corporation has recently included Voice Over IP (VoIP) in their corporate network. Unfortunately, the VoIP traffic also shares the wire with day-to-day traffic on a “Best Effort” network. Within a “Best Effort” environment, all traffic is treated equally and there is no differentiation in network service. In this environment, VoIP traffic would be sensitive to delays in packet transmission and packet loss often found with “Best Effort” delivery, resulting in poor voice quality between source and destination.

After careful examination of XYZ’s network traffic and hardware/software resources, a plan of action was developed. Upgrades in hardware/software revisions as required by their manufacturers and reconfiguration of portions of the network topology helped to improve transmission. However, XYZ’s network traffic still relied on “Best Effort” service and their VoIP applications continued to fall victim to network congestion during peak times.

Quality of Service (QoS) will offer the XYZ Corporation a way to provide a higher level of bandwidth to VoIP applications and other time-sensitive communication, while still providing delivery of the
remaining types of traffic within a reasonable timeframe. Thus, there is no need to overprovision the network bandwidth or build a parallel network for VoIP traffic.

**Components of DiffServ**

The following sections discuss the DiffServ environment from general concepts to more specific information, including the role of HP-UX IPQoS in that environment.

In the DiffServ model, packets are marked with a DiffServ Code Point (DSCP) value which corresponds to a specific traffic forwarding behavior referred to as a Per-Hop Behavior (PHB). The DSCP is set by the source DS node and/or DS Boundary node located primarily at the edges of a DS Domain. The Domain signifies a separate network or other administrative boundary of a DiffServ compliant environment. The PHBs in use can be those defined by IETF RFC standards\(^1\) or they can be locally defined.

![DiffServ Model Diagram](image)

In the above example, DS domains in each building of XYZ Corporation operate under different QoS policies and PHBs. A common set of policies will be needed at the DS boundary nodes to maintain the service requirements for applications such as VoIP communications.

**Traffic Classification and Conditioning**

As the packet enters the Boundary node it undergoes the process of Traffic Classification and Conditioning. The Traffic Classifier will direct the packets to Conditioners based on defined rules for the particular traffic type. Conditioning will evaluate the packets and determine what action if any needs to be taken on the packet to bring it into conformance within service level agreements.

**Classification**

The DiffServ model supports (2) types of Traffic Classifiers: Behavior Aggregate (BA) and the Multi-Field (MF) Aggregate. The BA classifies traffic based on the value of the DSCP. The MF Aggregate classifies packets based on multiple fields of the packet such as source or destination address(es) or

---

\(^1\) More information on standardized Per-Hop Behaviors can be found in RFC 2474 “Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers”, RFC 2597 “Assured Forwarding PHB Group”, and RFC 2598 “An Expedited Forward PHB”.
port numbers. Packets are grouped into traffic flows based on BA or MF filters to be forwarded in a pre-defined forwarding manner.

In our example, the XYZ Corporation will want to filter its VoIP traffic using one or more fields in the IP header. These fields may include source/destination addresses, ports, or protocol id. The VoIP application at XYZ uses the Real-Time Transport Protocol (RTP) to send data. RTP uses the UDP protocol and UDP port number which will be used in the QoS configuration when filtering the VoIP traffic.

Once the traffic has been classified (filtered) into like packet streams, the packets continue to the next phase, Traffic Conditioning.

Conditioning
Traffic conditioning can include functions for metering, (re)marking, and shaping/dropping. These functions bring packet streams into conformance (referred to as “in-profile”), if needed, to the agreed upon service levels. It may be required that non-conforming (“out-of-profile”) packets be delayed or dropped to satisfy the requirements for the particular traffic stream.

Metering
Metering measures the current state of a traffic stream against the expected state as defined by the traffic profile. The state information is then used to trigger any necessary actions by marking, shaping, and/or dropping.

Marking
Marking sets (or resets) the DS Codepoint in the leftmost 6-bits of the ToS field of the IPv4 header or the Traffic Class field in IPv6. The packet is then assigned to a traffic aggregate or traffic flow (referred to as a DS Behavior Aggregate) containing the same DSCP value. The DSCP value will map to a forwarding behavior defined by a PHB and will be applied to all traffic within that Behavior Aggregate. Several PHB standards exist today that define an “Assured Forwarding (AF) PHB Group” and “Expedited Forwarding (EF) PHB” (RFC’s 2597 and 2598). To ensure backwards compatibility with existing ToS values, refer to RFC 2474, “Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers”.

For the following IPv4 and IPv6 header diagrams, the DSCP value is shaded and the remaining 2-bits (currently unused) have been shaded with lines.
Shaping and Dropping (Policing)

Shaping is the process of delaying packets so that the traffic stream is brought into conformance with the specified profile. For example, a specific traffic stream may be allowed 30% of the bandwidth but, if left unchecked, could consume 50% of the bandwidth. Shaping would delay packets within the traffic stream to bring the maximum bandwidth to the defined limit of 30%.

Dropping (also referred to as Policing) is the process of discarding packets for the purpose of complying with defined traffic profiles.

(Note: the above diagram is not to scale.)
HP-UX IPQoS

HP-UX IPQoS conforms to IETF standards for the Differentiated Services architecture of QoS and provides traffic classification and conditioning. HP-UX IPQoS provides host-based functionality for outbound packets. It includes an administration tool, `ipqosadmin`, which can be used for loading, verifying, and unloading of configuration files as well as provide state and statistical information.

Configuration

HP-UX IPQoS operation loads a user modified configuration file that contains three distinct sections or blocks: Filter, Policy, and Adapter blocks.

General Example

The following example shows a pseudo-syntax configuration file with brief descriptions of each block type. This example, as well as other configuration file examples, can also be found in the HP-UX IPQoS Administrator’s Guide.

```
#######
# # Pseudo-Syntax Configuration File Example
#
filter filter1 {
    filter1_attributes
}
filter filter2 {
    filter2_attributes
}
policy policy1 {
    policy1_attributes
}
policy policy2 {
    policy2_attributes
}
adapter lanX {
    adapter_attributes
}
adapter lanY {
    adapter_attributes
}
# ######
```

Filters

Filters define specific traffic classes which can be based on BA Classifiers (DSCP) or Multi-Field (MF) Classifiers. HP-UX IPQoS supports both BA Classifiers and MF Classifiers and can classify on any combination of the following: IP source or destination address, name, or address range; source and/or destination port number, name, or port range; transport protocol number (TCP or UDP are currently supported); network protocol number (EtherType); DSCP value; and destination physical (MAC) address.

Policies

Policies specify actions to be taken on a particular traffic class defined in the Filter block such as bandwidth allocation or marking a DSCP value.
Adapters
Adapter blocks assign policies to specific configured adapters (NICs) on the system.

XYZ Configuration
XYZ has determined that they’ll reserve at least 40% of the bandwidth for VoIP communications. The remaining bandwidth will be used for all other communication. Using this information, the following configuration was implemented on their HP-UX systems and similar configurations propagated to their border routers:

```
# # Simple VoIP example configuration #
# Define Filters
#
filter voip_traffic_f
   port 7000
   protocol udp
   priority 1

# Define Policies
#
policy voip_traffic_p
   uses voip_traffic_f
   res 40%
   dscp 46

# Define Adapters
#
adapter lan0
   uses voip_traffic_p
```

In the above example, the filter voip_traffic_f identifies all communication received via UDP and port 7000 to apply the forwarding behavior defined in the policy voip_traffic_p. Adapter lan0 has been identified as the outgoing interface. You’ll note that “policy voip_traffic_p” lists “dscp 46”. The value “46” denotes that the packets are to receive Expedited Forwarding PHB (see RFC 2598, An Expedited Forwarding PHB for additional information). All other traffic which has not been defined in a QoS configuration will receive the Default PHB of Best Effort service subject to defined policies precedence.

Using DiffServ in their environment now allows XYZ Corporation to receive guaranteed bandwidth for their VoIP applications, reducing jitter and delays, for uninterrupted communication.

---

Note: The example is for illustration and that the protocols and port id’s used can vary with different VoIP applications. Check your VoIP product’s documentation for further information or for other possible classifiers.
Summary

Differentiated Services (also referred to as DiffServ or DS) provides a network administrator with the ability to classify network traffic by specific flows and to apply a traffic policy to each of those flows. Multimedia applications, for example, may need dedicated higher bandwidth to avoid jitter and delay to ensure seamless communications. Other types of traffic may have bandwidth requirements as well and would benefit from DiffServ.

HP-UX IPQoS provides a host-based implementation that works within your DiffServ environment for outbound traffic. HP-UX IPQoS conforms to IETF standards and supports bandwidth allocation, DSCP, and VLAN marking.

This white paper serves to provide only an introduction to the many features available with DiffServ and HP-UX IPQoS. Additional references for HP-UX IPQoS and IETF RFC’s are listed at the end of this document.
For More Information

Request for Comments

Request for Comments (RFCs) can be found at www.ietf.org

RFC 2474, Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers
RFC 2475, An Architecture for Differentiated Services
RFC 2597, Assured Forwarding PHB Group
RFC 2598, An Expedited Forwarding PHB
RFC 791, Internet Protocol
RFC 2460, Internet Protocol, Version 6 (IPv6)

Associated HP IP Quality of Service (IPQoS) documents

The following HP-UX IPQoS documents can be found at HP’s Documentation Web site, http://docs.hp.com/en/netcom.html#IPQos under the Networking and Communications collection.

- HP-UX IPQoS Administrator’s Guide
- HP-UX IPQoS Programmer’s Guide
- HP-UX IPQoS Release Notes