Network Working Group
Request for Comments: 4594
Category: Informational

J. Babiarz
K. Chan
Nortel Networks
F. Baker
Cisco Systems

August 2006

Configuration Guidelines for DiffServ Service Classes

Status of This Memo

Copyright Notice

Abstract

This document describes service classes configured with Diffserv and recommends how they can be used and how to construct them using Differentiated Services Code Points (DSCPs), traffic conditioners, Per-Hop Behaviors (PHBs), and Active Queue Management (AQM) mechanisms. There is no intrinsic requirement that particular DSCPs, traffic conditioners, PHBs, and AQM be used for a certain service class, but as a policy and for interoperability it is useful to apply them consistently.

Table of Contents

1. Introduction

To aid in understanding the role of this document, we use an analogy: the Differentiated Services specifications are fundamentally a toolkit. The specifications provide the equivalent of band saws, planers, drill presses, and other tools. In the hands of an expert, there is no limit to what can be built, but such a toolkit can be intimidating to the point of being inaccessible to a non-expert who just wants to build a bookcase. This document should be viewed as a set of "project plans" for building all the (diffserv) furniture that one might want. The user may choose what to build (e.g., perhaps our non-expert doesn't need a china cabinet right now), and how to go about building it (e.g., plans for a non-expert probably won't employ mortise/tenon construction, but that absence does not imply that mortise/tenon construction is forbidden or unsound). The authors hope that these diffserv "project plans" will provide a useful guide to Network Administrators in the use of diffserv techniques to implement quality-of-service measures appropriate for their network's traffic.

This document describes service classes configured with Diffserv and recommends how they can be used and how to construct them using Differentiated Services Code Points (DSCPs), traffic conditioners, Per-Hop Behaviors (PHBs), and Active Queue Management (AQM) mechanisms. There is no intrinsic requirement that particular DSCPs, traffic conditioners, PHBs, and AQM be used for a certain service class, but as a policy and for interoperability it is useful to apply them consistently.

Service class definitions are based on the different traffic characteristics and required performance of the applications/services. This approach allows us to map current and future applications/services of similar traffic characteristics and performance requirements into the same service class. Since the applications'/services' characteristics and required performance are end to end, the service class notion needs to be preserved end to end. With this approach, a limited set of service classes is required. For completeness, we have defined twelve different service classes, two for network operation/administration and ten for user/subscriber applications/services. However, we expect that network administrators will implement a subset of these classes

relevant to their customers and their service offerings. Network Administrators may also find it of value to add locally defined service classes, although these will not necessarily enjoy end-to-end properties of the same type.

Section 1 provides an introduction and overview of technologies that are used for service differentiation in IP networks. Section 2 is an overview of how service classes are constructed to provide service differentiation, with examples of deployment scenarios. Section 3 provides configuration guidelines of service classes that are used for stable operation and administration of the network. Section 4 provides configuration guidelines of service classes that are used for differentiation of user/subscriber traffic. Section 5 provides additional guidance on mapping different applications/protocols to service classes. Section 6 addresses security considerations.

1.1. Requirements Notation

The key words "SHOULD", "SHOULD NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

1.2. Expected Use in the Network

In the Internet today, corporate LANs and ISP WANs are generally not heavily utilized. They are commonly 10% utilized at most. For this reason, congestion, loss, and variation in delay within corporate LANs and ISP backbones is virtually unknown. This clashes with user perceptions, for three very good reasons.

- The industry moves through cycles of bandwidth boom and bandwidth bust, depending on prevailing market conditions and the periodic deployment of new bandwidth-hungry applications.
- In access networks, the state is often different. This may be because throughput rates are artificially limited or over-subscribed, or because of access network design trade-offs.
- Other characteristics, such as database design on web servers (that may create contention points, e.g., in filestore) and configuration of firewalls and routers, often look externally like a bandwidth limitation.

The intent of this document is to provide a consistent marking, conditioning, and packet treatment strategy so that it can be configured and put into service on any link that is itself congested.

1.3. Service Class Definition

A "service class" represents a set of traffic that requires specific delay, loss, and jitter characteristics from the network. Conceptually, a service class pertains to applications with similar characteristics and performance requirements, such as a "High-Throughput Data" service class for applications like the web and electronic mail, or a "Telephony" service class for real-time traffic such as voice and other telephony services. Such a service class may be defined locally in a Differentiated Services (DS) domain, or across multiple DS domains, possibly extending end to end.

A service class as defined here is essentially a statement of the required characteristics of a traffic aggregate. The required characteristics of these traffic aggregates can be realized by the use of defined per-hop behavior (PHB) [RFC2474]. The actual specification of the expected treatment of a traffic aggregate within a domain may also be defined as a per-domain behavior (PDB) [RFC3086].

Each domain may choose to implement different service classes or to use different behaviors to implement the service classes or to aggregate different kinds of traffic into the aggregates and still achieve their required characteristics. For example, low delay, loss, and jitter may be realized using the EF PHB, or with an over-provisioned AF PHB. This must be done with care as it may disrupt the end-to-end performance required by the applications/services. This document provides recommendations on usage of PHBs for specific service classes for their consistent implementation. These recommendations are not to be construed as prohibiting use of other PHBs that realize behaviors sufficient for the relevant class of traffic.

The Default Forwarding "Standard" service class is REQUIRED; all other service classes are OPTIONAL. It is expected that network administrators will base their choice of the level of service differentiation that they will support on their need, starting off with three or four service classes for user traffic and adding others as the need arises.

1.4. Key Differentiated Services Concepts

The reader SHOULD be familiar with the principles of the Differentiated Services Architecture [RFC2474]. We recapitulate key concepts here only to provide convenience for the reader, the referenced RFCs providing the authoritative definitions.

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.