

# Implementierung von Quality of Service-Richtlinien mit Differentiated Services Code Point

## Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konventionen](#)

[Hintergrundinformationen](#)

[Differentiated Services Code Point](#)

[Sichere Weiterleitung](#)

[Beschleunigte Weiterleitung](#)

[DSCP-Feld verwenden](#)

[Paketklassifizierung](#)

[Markierung](#)

[Verwendung der zugesicherten Zugriffsrates oder des klassenbasierten Policing](#)

[DSCP-kompatibel WRED](#)

[Bekanntes Problem in den Zügen der Cisco IOS Software 12.2](#)

[Zugehörige Informationen](#)

## Einleitung

Dieses Dokument beschreibt, wie Sie die Differentiated Services Code Point (DSCP) -Werte in Quality of Service (QoS)-Konfigurationen auf einem Cisco Router festlegen.

## Voraussetzungen

### Anforderungen

Sie müssen mit den Feldern im IP-Header und der Cisco IOS<sup>®</sup> CLI vertraut sein.

### Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

### Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter [Cisco Technical Tips Conventions](#).

## Hintergrundinformationen

Differentiated Services (DiffServ) ist ein neues Modell, bei dem der Datenverkehr von Zwischensystemen mit relativen Prioritäten behandelt wird, die auf dem ToS-Feld (Type of Services) basieren. Der [in RFC 2474](#) und [RFC 2475](#) definierte DiffServ-Standard ersetzt die ursprüngliche Spezifikation zur Definition der in [RFC 791](#) beschriebenen Paketpriorität. DiffServ erhöht die Anzahl der definierbaren Prioritätsstufen, wenn Bits eines IP-Pakets neu zugewiesen werden, um es als Priorität zu markieren.

Die DiffServ-Architektur definiert das DiffServ (DS)-Feld, das das ToS-Feld in IPv4 ersetzt, um Entscheidungen zum Verhalten pro Hop (PHB) bezüglich der Paketklassifizierung und des Datenverkehrs zu treffen `conditioning` Funktionen wie `metering`, `marking`, `shaping` und `policing`.

Die RFCs geben nicht vor, wie PHBs implementiert werden sollen. dafür ist der Anbieter verantwortlich. Implementierung durch Cisco `queuing` Techniken, die ihr PHB auf der IP-Rangfolge oder dem DSCP-Wert im IP-Header eines Pakets basieren können. Auf Basis des DSCP oder der IP-Rangfolge kann der Datenverkehr in eine bestimmte Serviceklasse geleitet werden. Pakete innerhalb einer Dienstklasse werden auf die gleiche Weise behandelt.

## Differentiated Services Code Point

Die sechs höchstwertigen Bits des DiffServ-Felds werden als DSCP bezeichnet. Die letzten beiden CU-Bits (Current Unused) im DiffServ-Feld wurden nicht in der DiffServ-Feldarchitektur definiert. Diese werden nun als Explicit Congestion Notification (ECN)-Bits verwendet. Router am Netzwerk-Edge klassifizieren Pakete und markieren sie mit der IP-Rangfolge oder dem DSCP-Wert in einem DiffServ-Netzwerk. Andere Netzwerkgeräte im Core, die Diffserv unterstützen, verwenden den DSCP-Wert im IP-Header, um ein PHB-Verhalten für das Paket auszuwählen und die entsprechende QoS-Behandlung bereitzustellen.

Die Diagramme in diesem Abschnitt zeigen einen Vergleich zwischen dem in [RFC 791](#) definierten ToS-Byte und dem DiffServ-Feld.

### ToS-Byte

P2

P1

P0

T2

T1

T0

Kupfer 1

CU

- IP-Rangfolge - drei Bit (P2 bis P0)
- Verzögerung, Durchsatz und Zuverlässigkeit - drei Bit (T2 bis T0)
- CU (Derzeit nicht verwendet) - zwei Bit (CU1-CU0)

### DiffServ-Feld

DS5 DS4 DS3 DS2 DS1 DS0 ECN ECN

- DSCP - sechs Bit (DS5-DS0)
- ECN - zwei Bit

Das standardisierte DiffServ-Feld des Pakets wird mit einem Wert markiert, sodass das Paket an jedem Netzknoten eine bestimmte Weiterleitungsverarbeitung oder PHB erhält.

Der Standard-DSCP ist 000 000. Klassenauswahl-DSCPs sind Werte, die abwärtskompatibel mit

der IP-Rangfolge sind. Wenn Sie zwischen IP-Rangfolge und DSCP konvertieren, wählen Sie die drei höchstwertigen Bits aus. So

IP Prec 5 (101) maps to IP DSCP 101 000

## ToS-Byte

1 0 1 T2 T1 T0 FE 2 CU0

## DiffServ-Feld

1 0 1 0 0 0 ECN ECN

Der DiffServ-Standard verwendet die gleichen Prioritätsbits (die signifikantesten Bits - DS5, DS4 und DS3) für die Prioritätseinstellung, präzisiert jedoch die Definitionen, wodurch eine feinere Granularität durch die Verwendung der nächsten drei Bits im DSCP erreicht wird. DiffServ ordnet die Prioritätsstufen (die immer noch durch die drei signifikantesten Bits des DSCP definiert sind) neu zu und benennt sie in diese Kategorien um (die Stufen werden in diesem Dokument genauer erläutert):

Rangfolge	Beschreibung
7	Bleibt unverändert (Link Layer und Routing Protocol Keepalive)
6	Bleibt gleich (wird für IP-Routing-Protokolle verwendet)
5	Express Forwarding (EF)
4	Klasse 4
3	Klasse 3
2	Klasse 2
1	Klasse 1
0	Beste Leistung

Bei diesem System priorisiert ein Gerät den Datenverkehr zuerst nach Klasse. Anschließend wird Datenverkehr der gleichen Klasse differenziert und priorisiert, wobei die Wahrscheinlichkeit eines Datenverlusts berücksichtigt wird.

Der DiffServ-Standard gibt keine präzise Definition der "niedrigen", "mittleren" und "hohen" Ausfallwahrscheinlichkeit vor. Nicht alle Geräte erkennen die DiffServ-Einstellungen (DS2 und DS1). und selbst wenn diese Einstellungen erkannt werden, lösen sie nicht notwendigerweise dieselbe PHB-Weiterleitungsaktion an jedem Netzwerkknoten aus. Jeder Knoten implementiert seine eigene Antwort auf Grundlage seiner Konfiguration.

## Zuversichtlich Forwarding

[RFC 2597](#) definiert die zugesicherte forwarding (AF) PHB und beschreibt es als ein Mittel für eine Provider-DS-Domäne, verschiedene forwarding Garantien für IP-Pakete, die von einer Client-DS-Domäne empfangen werden. Der sichere Forwarding PHB garantiert einer AF-Klasse eine bestimmte Bandbreite und ermöglicht den Zugriff auf zusätzliche Bandbreite, falls verfügbar. Es gibt vier AF-Klassen: AF1x bis AF4x. Innerhalb jeder Klasse gibt es drei Drop-Wahrscheinlichkeiten. Abhängig von einer bestimmten Netzwerkrichtlinie können Pakete für ein PHB basierend auf dem erforderlichen Durchsatz, Verzögerungen, Jitter, Verlust oder nach Zugriffspriorität für Netzwerkservices ausgewählt werden.

Die Klassen 1 bis 4 werden als AF-Klassen bezeichnet. Diese Tabelle zeigt den DSCP-Code, der die AF-Klasse mit der Wahrscheinlichkeit angibt. Die Bits DS5, DS4 und DS3 definieren die Klasse. Die Bits DS2 und DS1 geben die Tropfwahrscheinlichkeit an; Bit DS0 ist immer Null.

Löschen	Klasse 1	Klasse 2	Klasse 3	Klasse 4
Niedrig	001010 AF11 DSCP 10	010010 AF21 DSCP 18	011010 AF31 DSCP 26	100010 AF41 DSCP 34
Mittel	001100 AF12 DSCP 12	010100 AF 22 DSCP 20	011100 AF32 DSCP 28	100100 AF42 DSCP 36
Hoch	001110 AF13 DSCP 14	010110 AF23 DSCP 22	011110 AF33 DSCP 30	100110 AF43 DSCP 38

## Beschleunigt Forwarding

[RFC 2598](#) definiert das Expedited Forwarding (EF) PHB: "Das EF PHB kann verwendet werden, um einen End-to-End-Service mit geringem Verlust, geringer Latenz, geringem Jitter und zugesicherter Bandbreite über DS (Diffserv)-Domänen zu erstellen. Ein solcher Service erscheint den Endpunkten wie eine Punkt-zu-Punkt-Verbindung oder eine "virtuelle Mietleitung". Dieser Service wird auch als Premium-Service bezeichnet. Für das EF-PHB wird der Codepoint 101110 empfohlen, was einem DSCP-Wert von 46 entspricht.

Auch hier müssen anbieterspezifische Mechanismen konfiguriert werden, um diese PHBs zu implementieren. Weitere Informationen zu EF PHB finden Sie in [RFC 2598](#).

## DSCP-Feld verwenden

Das DSCP-Feld kann auf drei Arten verwendet werden:

- Classifier (Klassifizierung): Wählen Sie ein Paket basierend auf dem Inhalt einiger Teile des Paket-Headers aus, und wenden Sie PHB basierend auf den durch den DSCP-Wert definierten Service-Merkmalen an.
- Marker - Das DSCP-Feld wird auf Basis des Datenverkehrsprofils festgelegt.
- Metering - Überprüfen Sie die Konformität mit dem Datenverkehrsprofil mit einer Shaper- oder Dropper-Funktion.

Die Cisco IOS-Software berücksichtigt die Prioritätsbits des ToS-Felds, wenn Datenverkehr in die Warteschlange für Weighted Fair Queuing (WFQ), Weighted Random Early Detection (WRED) oder Weighted Round Robin (WRR) gestellt wird. Die Prioritätsbits werden nicht berücksichtigt, wenn Policy Routing, Priority Queuing (PQ), Custom Queuing (CQ) oder Class Based Weighted Fair Queuing (CBWFQ) konfiguriert sind. Weitere Informationen finden Sie unter [Class Based Weighted Fair Queuing \(CBWFQ\)](#).

## Paketklassifizierung

Die Paketklassifizierung beinhaltet die Verwendung eines Datenverkehrsdeskriptors, um ein Paket innerhalb einer bestimmten Gruppe zu kategorisieren und es für die im Netzwerk verwaltete QoS zugänglich zu machen. Bei der Paketklassifizierung können Sie den Netzwerkverkehr in mehrere Prioritätsstufen oder eine Class of Service (CoS) unterteilen.

Sie können entweder Zugriffslisten (ACLs) oder den Befehl **match** in der modularen QoS-CLI verwenden, um DSCP-Werte abzugleichen. Seit Version 12.1(5)T der Cisco IOS-Software besteht die Möglichkeit, im Match-Befehl einen DSCP-Wert auszuwählen.

```

Router1(config)#access-list 101 permit ip any any ?
dscp          Match packets with given dscp value
fragments    Check non-initial fragments
log          Log matches against this entry
log-input    Log matches against this entry, including input interface
precedence   Match packets with given precedence value
time-range   Specify a time-range
tos          Match packets with given TOS value

```

Wenn Sie den *ip dscp*-Wert im **Klassenzuordnungsbefehl** angeben, haben Sie folgende Möglichkeiten:

```

Router(config)#class-map match-all VOIP
1751-uut1(config-cmap)#match ip dscp ?
<0-63>      Differentiated services codepoint value
af11        Match packets with AF11 dscp (001010)
af12        Match packets with AF12 dscp (001100)
af13        Match packets with AF13 dscp (001110)
af21        Match packets with AF21 dscp (010010)
af22        Match packets with AF22 dscp (010100)
af23        Match packets with AF23 dscp (010110)
af31        Match packets with AF31 dscp (011010)
af32        Match packets with AF32 dscp (011100)
af33        Match packets with AF33 dscp (011110)
af41        Match packets with AF41 dscp (100010)
af42        Match packets with AF42 dscp (100100)
af43        Match packets with AF43 dscp (100110)
cs1         Match packets with CS1(precedence 1) dscp (001000)
cs2         Match packets with CS2(precedence 2) dscp (010000)
cs3         Match packets with CS3(precedence 3) dscp (011000)
cs4         Match packets with CS4(precedence 4) dscp (100000)
cs5         Match packets with CS5(precedence 5) dscp (101000)
cs6         Match packets with CS6(precedence 6) dscp (110000)
cs7         Match packets with CS7(precedence 7) dscp (111000)
default     Match packets with default dscp (000000)
ef          Match packets with EF dscp (101110)
Router1(config-cmap)#match ip dscp af31

```

## Marking

Der DSCP kann am Netzwerk-Edge auf einen gewünschten Wert eingestellt werden, damit Core-Geräte das Paket, wie im Abschnitt zur [Paketklassifizierung](#) dargestellt, auf einfache Weise klassifizieren und ein geeignetes Servicelevel bereitstellen können. [Klassenbasiertes Paket Marking](#) kann verwendet werden, um den DSCP-Wert wie folgt festzulegen:

```
policy-map pack-multimedia-5M
```

```

!--- Creates a policy map named pack-multimedia-5M. class management !--- Specifies the policy
to be created for the !--- traffic classified by class management. bandwidth 50 set ip dscp 8 !-
-- Sets the DSCP value of the packets matching !--- class management to 8. class C1 priority
1248 set ip dscp 40 class voice-signalling bandwidth 120 set ip dscp 24

```

## Verwendung der zugesicherten Zugriffsrates oder des klassenbasierten Policing

Committed Access Rate und Class-Based Policing sind Verkehrsregelungsmechanismen, die den Verkehrsfluss entsprechend der vereinbarten Dienstparameter regeln. Diese Mechanismen können zusammen mit DSCP verwendet werden, um verschiedene Service-Level bereitzustellen, die nicht dem Datenverkehr entsprechen und dies auch tun, wenn der DSCP-Wert entsprechend geändert wird, wie in diesem Abschnitt gezeigt.

Siehe [Configuring Datenverkehr Policing](#) und [Vergleich von klassenbasiertem Policing und Committed Access Rate](#).

```
interface Serial1/0.1 point-to-point
 bandwidth 5000
 ip address 192.168.126.134 255.255.255.252
 rate-limit output access-group 150 8000 1500 2000 conform-action
   set-dscp-transmit 10 exceed-action set-dscp-transmit 20
```

```
!--- For traffic matching access list 150, sets the DSCP value of conforming traffic !--- to 10
and that of non-conforming traffic to 20. rate-limit output access-group 152 8000 1500 2000
conform-action set-dscp-transmit 15 exceed-action set-dscp-transmit 25 rate-limit output access-
group 154 8000 1500 2000 conform-action set-dscp-transmit 18 exceed-action set-dscp-transmit 28
frame-relay interface-dlci 17 class shaper-multimedia-5M
```

## DSCP-kompatibel WRED

Weighted Random Early Detection (WRED): Verwirft selektiv Datenverkehr mit niedrigerer Priorität, wenn die Schnittstelle überlastet wird. WRED kann differenzierte Leistungsmerkmale für verschiedene CoS bieten. Dieser differenzierte Service kann auf Grundlage des DSCP bereitgestellt werden, wie hier gezeigt:

```
class C2
 bandwidth 1750
 random-detect dscp-based
```

```
!--- Enable dscp-based WRED as drop policy. random-detect exponential-weighting-constant 7 !---
Specifies the exponential weight factor for the !--- average queue size calculation for the
queue. random-detect dscp 16 48 145 10 !--- Specifies the minimum and maximum queue thresholds
!--- for each DSCP value. random-detect dscp 32 145 435 10
```

Weitere Informationen finden Sie im Abschnitt [Übersicht](#) zur [Überlastungsvermeidung](#) unter [WRED, der](#) mit DiffServ konform ist.

## Bekannte Probleme in den Zügen der Cisco IOS Software 12.2

Der Zugriff auf Bug-Tools und -Informationen ist nur für registrierte Cisco Kunden möglich.

Sie können diese Fehler mit dem [Bug Search Tool](#) suchen.

- Cisco Bug-ID [CSCdt63295](#) - Wenn das ToS-Byte mit dem neuen DSCP nicht festgelegt werden kann marking-Befehlen auf den DFÜ-Peers (auf 0 gesetzt) in Cisco IOS Software, Version 12.2.2T, können Pakete nicht markiert werden und sie können mit einem ToS von 0 erhalten bleiben.
- Cisco Bug-ID [CSCdt74738](#): Die Unterstützung für den Befehl **set ip dscp** auf dem Cisco 7200-Router und den Plattformen der unteren Leistungsklasse für Multicast-Pakete muss ab Cisco IOS Software, Version 12.2(3.6) und höher, verfügbar sein.

## Zugehörige Informationen

- [Cisco IOS Software: Netzwerklösungen für Service Provider](#)
- [Technischer Support – Cisco Systems](#)
- [QoS: Konfigurationsleitfaden zur Überlastungsvermeidung](#)

## Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.