Revised: November 2, 2026

Configure DSCP and QoS Traffic Scheduling on Cisco Secure Routers using Cisco Meraki Dashboard

Feature history of DSCP and QoS traffic scheduling

Table 1: Feature history table

Feature	Release	Description
DSCP Tagging, Quality of Service, and Traffic Scheduling	Cisco IOS XE 26.2.1 Release	From this release, Cisco 8000 Series Secure Routers can be configured for traffic scheduling using Cisco Meraki Dashboard.

DSCP tagging, Quality of Service, and traffic scheduling

Quality of Service (QoS) and traffic scheduling control how traffic is marked, classified, and served when a WAN link is congested. DSCP tagging writes a Differentiated Services Code Point value into the IP header. The router uses the resulting DSCP value to place traffic into a fixed forwarding queue.

The configuration has two parts:

- Ingress remarking matches traffic and assigns a DSCP value.
- Egress queuing classifies DSCP-marked traffic and schedules it on the WAN interface.

This feature extends the traffic-shaping model used for Cisco Meraki MX networks to Cisco Secure Routers. Traffic-shaping rules do not apply to traffic sent over a non Cisco Meraki VPN tunnel.

Traffic can be matched by a Meraki application, application category, port, or IP range. A matching rule assigns a DSCP value. The assigned value determines the forwarding priority and queue used by the egress QoS policy.

The default egress scheduler uses four effective queues:

- Realtime: strict priority treatment with 50 percent priority bandwidth.
- High: bandwidth remaining ratio 4.
- Medium: the `class-default` queue, with bandwidth remaining ratio 2.
- Low: bandwidth remaining ratio 1.

The scheduler's bandwidth percentages shown in the release material are approximately 50 percent for Realtime, 28.6 percent for High, 14.3 percent for Medium, and 7.1 percent for Low.

Restrictions for DSCP and QoS traffic scheduling

- Explicit dashboard rule-level `Priority` is unsupported on Cisco Secure Routers.
- Per-client bandwidth limiting is unsupported on Cisco Secure Routers.
- The dashboard does not use a per-WAN-uplink maximum bandwidth value for Cisco Secure Routers; the fallback behavior uses 100 percent or automatic uplink bandwidth.

- Hostname definitions are not supported in the Traffic-shaping rules.
- The Meraki applications which are not supported on Cisco Secure Routers are skipped by the Cisco Meraki Dashboard.
- For Cisco Secure Router networks, the supported directional custom-expression types are source, destination, source_port, and destination_port. The existing net, net/port, port, and localnet expression types are not supported for these networks. MX network behavior remains unchanged.
- Only IPv4 addresses are supported.
- A rule whose DSCP setting is "Do not change DSCP tag" retains the matched traffic existing ingress DSCP value and generates no DSCP marking action, preventing the lower ranked rules with with same/overlapping matched traffic from overriding the matched traffic existing DSCP tag.
- Each selected Dashboard application category is expanded into its mapped applications before CLI generation. Application matchers are grouped into class-maps of no more than 32 matcher references.
- A non-hierarchical IOS-XE class-map supports up to 32 match statements. For a hierarchical class-map, the combined number of match statements in the parent and its child class-maps must not exceed 96. Dashboard batches category and rule class-maps to satisfy both limits.
- Dashboard generates application and application-category NBAR configuration for both default and user-defined Traffic Shaping rules on Cisco Secure Router networks.

Configure DSCP and QoS traffic scheduling

Choose one of the options to configure DSCP tagging, Quality of Service, and traffic scheduling

- DSCP tagging, Quality of Service, and traffic scheduling configuration using Cisco Meraki Dashboard
- DSCP tagging, Quality of Service, and traffic scheduling using Cisco Secure Routers

Configure DSCP Tagging, Quality of Service, and Traffic Scheduling on Cisco Meraki Dashboard

For information on configuring this feature on Cisco Meraki Dashboard, refer to SD-WAN and Traffic Shaping.

Step 1 From the Cisco Meraki Dashboard, navigate to **Security & SD-WAN** > **Configure** > **SD-WAN & Traffic shaping**.

Step 2 Select **Create a new rule**.

If rules already exist, select **Add a new shaping rule**.

Step 3 Define the traffic to match.

The workflow supports application categories and custom expressions such as ports and IP ranges.

Step 4 Configure the DSCP tagging value for the rule.

Step 5 Click **Save changes**.

Step 6 Return to **Security & SD-WAN** > **Configure** > **SD-WAN & Traffic shaping** and confirm that the rule displays the expected DSCP tagging setting.

Configure DSCP and QoS traffic scheduling on Cisco Secure Routers

Note

The router configurations are not manually set on the router, instead, all the configurations are automatically pushed from the Cisco Meraki cloud.

Dashboard-generated CLI naming

Egress queue class-map and policy-map names are fixed: TS_REALTIME_QUEUE, TS_HIGH_QUEUE, TS_LOW_QUEUE, TS_WAN_QOS_POLICY, TRAFFIC_SHAPING_POLICY_WAN1, and TRAFFIC_SHAPING_POLICY_WAN2.

The ingress DSCP remarking policy-map name is fixed as TS_INGRESS_REMARKING_POLICY. The four default ingress rule class-map names are fixed as TS_DEFAULT_EF, TS_DEFAULT_AF11, TS_DEFAULT_AF41, and TS_DEFAULT_AF21.

For each user-defined rule, Cisco Meraki Dashboard generates rule class-map names using the following batched, hash-suffixed format:

TS_R<rule_index> B<batch_index> <batch_matchers_sha256_hash>

When a user-defined rule's derived matcher set exceeds the class-map exceeds the class-map restriction of match statements, Dashboard splits the rule into multiple batched class-maps. The hash suffix uses the first 32 hex characters of a SHA-256 hash derived from the matcher references in that specific batch, so a class-map name changes when that batch's matcher set changes.

Configure the egress queues

Apply the following QoS policy to the WAN interfaces. The class-default entry is the effective Medium queue for DSCP values not matched by the explicit Realtime, High, or Low class maps.

```
!----Start---- Egress Queueing Config ----Start----
!
class-map match-any TS_REALTIME_QUEUE
 match dscp cs4
 match dscp af41
 match dscp af42
 match dscp af43
 match dscp cs5
 match dscp ef
 match dscp cs6
 match dscp 44
 match dscp cs7
 match dscp 33
 match dscp 35
 match dscp 37
 match dscp 39
 match dscp 41
 match dscp 42
 match dscp 43
 match dscp 45
 match dscp 47
 match dscp 49
 match dscp 50
 match dscp 51
 match dscp 52
 match dscp 53
 match dscp 54
 match dscp 55
 match dscp 57
 match dscp 58
 match dscp 59
 match dscp 60
 match dscp 61
 match dscp 62
 match dscp 63
!
```

```
class-map match-any TS_HIGH_QUEUE
 match dscp cs3
 match dscp af31
 match dscp af32
 match dscp af33
 match dscp 25
 match dscp 27
 match dscp 29
 match dscp 31
! Low-queue also matches packets with the "default" DSCP tag, which maps to DSCP value 0/cs0
class-map match-any TS_LOW_QUEUE
 match dscp default
 match dscp 1
 match dscp 2
 match dscp 3
 match dscp 4
 match dscp 5
 match dscp 6
 match dscp 7
!
!
policy-map TS_WAN_QOS_POLICY
 class TS_REALTIME_QUEUE
  priority percent 50
 class TS_HIGH_QUEUE
  bandwidth remaining ratio 4
 class TS_LOW_QUEUE
  bandwidth remaining ratio 1
! class-default is the effective Medium queue class for packets not
! matched by the explicit queue class-maps (ie, packets with remaining DSCP tags
! like af11,af12,af13,af21,af22,af23,cs1,cs2,cs7, etc.)
 class class-default
  bandwidth remaining ratio 2
!
!
policy-map TRAFFIC_SHAPING_POLICY_WAN1
 class class-default
  shape average percent 100
  service-policy TS_WAN_QOS_POLICY
!
policy-map TRAFFIC_SHAPING_POLICY_WAN2
 class class-default
  shape average percent 100
  service-policy TS_WAN_QOS_POLICY
!
!
! Physical WANs and WANs with tagged Vlans
! Egress Traffic Shaping policies will be attached to Physical WAN
! interfaces and WAN interfaces with tagged Vlans:
interface TenGigabitEthernet0/0/8
 ...
 service-policy output TRAFFIC_SHAPING_POLICY_WAN2
!
interface TenGigabitEthernet0/0/9.101
 ...
 service-policy output TRAFFIC_SHAPING_POLICY_WAN1
!----End---- Egress Queueing Config ----End----
```

Configure ingress DSCP remarking

Create class maps for the traffic that should be remarked, then assign DSCP values in the ingress policy. The following example shows the default rule classes and the DSCP assignments documented for the feature.

```
! ----Start---- default rules TrafficShaperClass.default_shape_configs
! when ssid.default_traffic_shapes_enabled ----Start----
!
!
! Ignored/Excluded Meraki specific Nbar apps unavailable in default protocol pack.
! Unresolved apps Nbar Ids: 2801, 2827, 3032, 3122, 3219, 3416
! Unresolved apps Nbar CLI names: Allscripts, Cerner, CureMD, Epic EHR, GE Healthcare, McKesson
class-map match-any TS_APP_CAT22
 match protocol dicom
 match protocol Epic EHR
!
! Ignored/Excluded Meraki specific Nbar apps unavailable in default protocol pack.
! Unresolved apps Nbar Ids: 2691, 2709, 3083, 3203, 3264, 3459, 3461
! Unresolved apps Nbar CLI names: adobe updates, bitdefender, eset, kaspersky, sophos, symantec,
webrootcloudav.com
class-map match-any TS_APP_CAT12
 match protocol android-updates
 match protocol mcafee-antivirus
 match protocol mcafee-update
 match protocol apple-app-store
 match protocol apple-updates
 match protocol apple-ios-updates
 match protocol apple-tv-updates
 match protocol google-downloads
 match protocol google-play
 match protocol java-web-portal
 match protocol mac-os-x-updates
 match protocol windows-store
 match protocol ms-update
!
! Ignored/Excluded Meraki specific Nbar apps unavailable in default protocol pack.
! Unresolved apps Nbar Ids: 2628, 2838, 3192, 3278
! Unresolved apps Nbar CLI names: Backblaze, Carbonite, IBackup, Mozy
class-map match-any TS_APP_CAT7
 match protocol backup-service
 match protocol connected-backup
 match protocol crashplan
 match protocol novastorbakcup
 match protocol td-replica
 match protocol tapeware
 match protocol icloud
!
! Ignored/Excluded Meraki specific Nbar apps unavailable in default protocol pack.
! Unresolved apps Nbar Ids: 2828, 2836, 3178
! Unresolved apps Nbar CLI names: BBC iPlayer, HBO GO, Miscellaneous video
class-map match-any TS_APP_CAT13_B1
 match protocol airplay
 match protocol amazon-instant-video
 match protocol appleqtc
 match protocol brighttalk
 match protocol directv-catlg
 match protocol directv-web
 match protocol disney-web-portal
 match protocol flash-video
 match protocol flashyahoo
 match protocol foodnetwork
 match protocol gyao
 match protocol keyholetv
 match protocol kuro
 match protocol letv-com
 match protocol livestation
 match protocol mpeg2-ts
 match protocol mtv
```

```
 match protocol ms-stream
 match protocol napster
 match protocol netflix
 match protocol nico-video
 match protocol pptv
 match protocol ppstream
 match protocol pandora
 match protocol pbs-web-portal
 match protocol qqlive
 match protocol rdt
 match protocol rtmpe
 match protocol rtmpt
 match protocol realmedia
 match protocol rhapsody
 match protocol sling
!
class-map match-any TS_APP_CAT13_B2
 match protocol sopcast
 match protocol soribada
 match protocol spotify
 match protocol ted
 match protocol tudou
 match protocol twitch-tv
 match protocol vimeo
 match protocol xunlei-kankan
 match protocol youtube
 match protocol youku
 match protocol zattoo
 match protocol hulu
 match protocol itunes
 match protocol itunes-media
 match protocol itunes-audio
 match protocol itunes-video
 match protocol megavideo
!
!
class-map match-any TS_DEFAULT_EF
 match protocol sip
!
class-map match-any TS_DEFAULT_AF11
 match class-map TS_APP_CAT22
 match class-map TS_APP_CAT12
 match class-map TS_APP_CAT7
!
class-map match-any TS_DEFAULT_AF41
 match protocol webex-media
 match protocol skype
!
class-map match-any TS_DEFAULT_AF21
 match class-map TS_APP_CAT13_B1
 match class-map TS_APP_CAT13_B2
!
!
! when ssid.default_traffic_shapes_enabled ----End----
! ----End---- default rules TrafficShaperClass.default_shape_configs

! ----Start---- User custom Rules mapped TrafficShaperClasses configs ----Start----
! ApplicationCategory id=3 name="File sharing" expanded Applications Group1
! Ignored/Excluded Meraki specific Nbar apps unavailable in default protocol pack.
! Unresolved apps Nbar Ids: 2559, 2959
! Unresolved apps Nbar CLI names: Mega, PutLocker.com
class-map match-any TS_APP_CAT3_B1
 match protocol afpovertcp
 match protocol box
```

```
 match protocol dropbox
 match protocol ftp-data
 match protocol fix
 match protocol gsiftp
 match protocol google-photos
 match protocol gtalk-ft
 match protocol gridftp
 match protocol hangouts-file-transfer
 match protocol onedrive
 match protocol skydrive
 match protocol microsoftds
 match protocol mftp
 match protocol ni-ftp
 match protocol netapp-snapmirror
 match protocol nfs
 match protocol oscar-filetransfer
 match protocol pftp
 match protocol prospero
 match protocol remotefs
 match protocol sst
 match protocol ftps-data
 match protocol sift-uft
 match protocol saft
 match protocol sftp
 match protocol softros-messenger-ft
 match protocol tftp
 match protocol tus-files
 match protocol uucp-path
 match protocol cifs
 match protocol secure-ftp
! ApplicationCategory id=3 name="File sharing" expanded Applications Group2
class-map match-any TS_APP_CAT3_B2
 match protocol rsync
!
! ApplicationCategory id=24 name="Databases & cloud services" expanded Applications Group1
! Ignored/Excluded Meraki specific Nbar apps unavailable in default protocol pack.
! Unresolved apps Nbar Ids: 2740, 2796, 3092, 3382
! Unresolved apps Nbar CLI names: Amazon RDS, Amazon Redshift, IBM Cloud, Sap Cloud Platform
class-map match-any TS_APP_CAT24_B1
 match protocol amazon-cloudfront
 match protocol Amazon RDS
 match protocol Amazon Redshift
 match protocol amazon-s3
 match protocol amazon-web-services
 match protocol windows-azure
 match protocol cassandra
 match protocol db-service
 match protocol ddm-dfm
 match protocol ddm-rdb
 match protocol ddm-ssl
 match protocol gds_db
 match protocol IBM Cloud
 match protocol sqlexec
 match protocol ibm-db2
 match protocol ingres-net
 match protocol ms-olap
 match protocol ms-sql-m
 match protocol sqlserver
 match protocol oracle-bi
 match protocol oraclenames
 match protocol net8-cman
 match protocol oraclenet8cman
 match protocol rdb-dbs-disp
 match protocol ora-srv
```

```
 match protocol coauthor
 match protocol mumps
 match protocol sqlserv
 match protocol rda
 match protocol Sap Cloud Platform
 match protocol sqlsrv
 match protocol oracle-sqlnet
! ApplicationCategory id=24 name="Databases & cloud services" expanded Applications Group2
class-map match-any TS_APP_CAT24_B2
 match protocol z39.50
 match protocol dbase
 match protocol mongo
 match protocol mysql
 match protocol tlisrv
 match protocol postgresql
!
! If rule definition matchers set exceeds CCE 32 matchers and 192-term RPN limit,
! then multiple rule class-maps would be generated TS_R1_B1_7A3F2E4C9B10D6A8F01C223344556677,
TS_R1_B2_6T3F2E4C9B10D6A8F01C223344556644, etc.
class-map match-any TS_R1_B1_7A3F2E4C9B10D6A8F01C223344556677
 match protocol citrix-audio
 match protocol cnn
 match class-map TS_APP_CAT3_B1
 match class-map TS_APP_CAT3_B2
 match class-map TS_APP_CAT24_B1
 match class-map TS_APP_CAT24_B2
!
!
ip access-list extended TS_R2_ACL
 10 permit tcp any any eq 9090
 20 permit udp any any eq 9090
 30 permit tcp any eq 9090 any
 40 permit udp any eq 9090 any
 50 permit tcp any any range 8000 9000
 60 permit udp any any range 8000 9000
 70 permit tcp any range 8000 9000 any
 80 permit udp any range 8000 9000 any
 90 permit tcp any 0.1.0.0 0.0.255.255 eq 80
 100 permit udp any 0.1.0.0 0.0.255.255 eq 80
 110 permit tcp 0.1.0.0 0.0.255.255 eq 80 any
 120 permit udp 0.1.0.0 0.0.255.255 eq 80 any
 130 permit ip any 192.1.0.0 0.0.255.255
 140 permit ip 192.1.0.0 0.0.255.255 any
 150 permit tcp any 192.168.0.0 0.0.255.255 range 2000 3000
 160 permit udp any 192.168.0.0 0.0.255.255 range 2000 3000
 170 permit tcp 192.168.0.0 0.0.255.255 range 2000 3000 any
 180 permit udp 192.168.0.0 0.0.255.255 range 2000 3000 any
! ApplicationCategory id=2 name="Blogging" expanded Applications Group1
! Ignored/Excluded Meraki specific Nbar apps unavailable in default protocol pack.
! Unresolved apps Nbar Ids: 3444
! Unresolved apps Nbar CLI names: WordPress
class-map match-any TS_APP_CAT2
 match protocol ameba
 match protocol blogger
 match protocol independent-news
 match protocol fc2
 match protocol jimdo
 match protocol weibo
 match protocol tianya
 match protocol typepad
!
class-map match-any TS_R2_B1_91E0A41B882C7711D3F95A06BC12AA09
 match access-group name TS_R2_ACL
 match class-map TS_APP_CAT2
```

```
 match protocol hotmail
!
!
ip access-list extended TS_R3_ACL
 10 permit tcp any any eq 9090
 20 permit udp any any eq 9090
 30 permit tcp any eq 9090 any
 40 permit udp any eq 9090 any
 50 permit ip any 192.1.0.0 0.0.255.255
 60 permit ip 192.1.0.0 0.0.255.255 any
 70 permit tcp any 10.1.0.0 0.0.255.255 eq 80
 80 permit udp any 10.1.0.0 0.0.255.255 eq 80
 90 permit tcp 10.1.0.0 0.0.255.255 eq 80 any
 100 permit udp 10.1.0.0 0.0.255.255 eq 80 any
!
class-map match-any TS_R3_B1_0F6D88C14E93BBA77D01245A09E7C331
 match access-group name TS_R3_ACL
!
! ----End---- User custom mapped TrafficShaperClasses configs ----End----


! ----Start---- Default + User custom Rules DSCP tagging ----Start----
policy-map TS_INGRESS_REMARKING_POLICY
 class TS_R1_B1_7A3F2E4C9B10D6A8F01C223344556677
  set dscp af11
! If Rule 1 definitions matchers were split to multiple top-level class-maps, then all
! such rule class-map entries with same rule DSCP mapping actions would be generated
! class TS_R1_B1_7A3F2E4C9B10D6A8F01C223344556677
!  set dscp af11
! class TS_R1_B2_6T3F2E4C9B10D6A8F01C223344556644
!  set dscp af11
 class TS_R2_B1_91E0A41B882C7711D3F95A06BC12AA09
  set dscp cs4
 class TS_R3_B1_0F6D88C14E93BBA77D01245A09E7C331
  set dscp af23
class TS_DEFAULT_EF
  set dscp ef
 class TS_DEFAULT_AF11
  set dscp af11
 class TS_DEFAULT_AF41
  set dscp af41
 class TS_DEFAULT_AF21
  set dscp af21
! ----End---- Default + User custom Rules DSCP tagging ----End----


!----Start---- Attach Ingress Policy-Map to aplicable interfaces ----Start----
! Physical L3 LANs, L3 LAN subinterfaces, VLANs and LACP Port-Channels
! Ingress QoS policy will be attached to all applicable physical L3 LANs, L3 LAN subinterfaces, VLANs
interface GigabitEthernet0/0/3
 ...
 service-policy input TS_INGRESS_REMARKING_POLICY
interface GigabitEthernet0/0/4.102
 ...
 service-policy input TS_INGRESS_REMARKING_POLICY
interface Vlan1
 ...
 service-policy input TS_INGRESS_REMARKING_POLICY
!
! Ingress QoS policy will also be attached to all applicable QoS aggregate mode LACP Port-Channels
platform qos port-channel-aggregate 1
interface Port-channel1
 ...
 service-policy input TS_INGRESS_REMARKING_POLICY
```

```
!
!
!----End---- Attach Ingress Policy-Map to aplicable interfaces ----End----
```

Supported rule matchers and class-map generation

A rule class-map can contain three matcher types: Dashboard application-category class-map matchers, ACL matchers, and direct application matchers.

Examples are match class-map TS_APP_CAT3 for an application-category class-map matcher, match access-group name TS_R2_ACL for an ACL matcher, and match protocol hotmail for a direct application matcher.

The preferred generated structure uses two levels. Application-category child class-maps contain batches of mapped application protocol matchers. The top-level rule class-map combines application-category class-map matchers, ACL matchers, and direct application matchers.

If the top-level rule matcher set exceeds the supported class-map limits, Dashboard generates multiple top-level rule class-maps and applies the same DSCP remarking action to each batch under TS_INGRESS_REMARKING_POLICY.

Add a custom traffic expressions rule

For a custom rule, create an ACL, reference it from a match-any class map, and add a DSCP assignment to the ingress policy. This example matches TCP/UDP port 9090 and assigns AF23.

```
ip access-list extended TS_R3_ACL
  10 permit tcp any any eq 9090
  20 permit udp any any eq 9090
!
class-map match-any TS_R3
  match access-group name TS_R3_ACL
!
policy-map TS_INGRESS_REMARKING_POLICY
  class TS_R3
    set dscp af23
```

Keep the order of classes in the ingress policy aligned with the order of traffic-shaping rules configured in Dashboard. If a rule has more than 32 matchers, the source material states that multiple class maps can be generated for that rule.

Verify DSCP and QoS traffic scheduling configurations

Use the 'show policy-map interface' command to show QoS details on a specific interface and the 'show policy-map target' command to show details on all interfaces:

Verify generated configuration names and matchers

In addition to verifying policy-map counters, confirm that the generated configuration contains the fixed egress names and TS_INGRESS_REMARKING_POLICY.

Confirm that user-defined rules use TS_R<rule#index>_B<rule_batch#index>_<batch_matchers_SHA256Hash>, and that application categories use TS_APP_CAT<DashboardCategory#Id>_B<DashboardCategory_batch#index>.

Confirm that rule class-maps use only application-category class-map matchers, ACL matchers, and direct application matchers.

Confirm that rules set to Do not change DSCP tag do not generate configuration when they have no other supported Cisco Secure Router effect.

QoS policy output

```
Router#show policy-map interface TenGigabitEthernet0/0/8
 TenGigabitEthernet0/0/8
  Service-policy output: TRAFFIC_SHAPING_POLICY_WAN1
    Class-map: class-default (match-any)
      4 packets, 240 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: any
      Queueing
      queue limit 1041 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 4/240
      shape (average) cir 1000000000, bc 10000000, be 10000000
      target shape rate 1000000000
      Service-policy : TS_WAN_QOS_POLICY
        queue stats for all priority classes:
          Queueing
          queue limit 512 packets
          (queue depth/total drops/no-buffer drops) 0/0/0
          (pkts output/bytes output) 0/0
        Class-map: TS_REALTIME_QUEUE (match-any)
          0 packets, 0 bytes
          5 minute offered rate 0000 bps, drop rate 0000 bps
          Match:  dscp cs4 (32)
          Match:  dscp af41 (34)
          Match:  dscp af42 (36)
          Match:  dscp af43 (38)
          Match:  dscp cs5 (40)
          Match:  dscp 44
          Match:  dscp ef (46)
          Match:  dscp cs6 (48)
          Priority: 50% (500000 kbps), burst bytes 12500000, b/w exceed drops: 0
        Class-map: TS_HIGH_QUEUE (match-any)
          0 packets, 0 bytes
          5 minute offered rate 0000 bps, drop rate 0000 bps
          Match:  dscp cs3 (24)
          Match:  dscp af31 (26)
          Match:  dscp af32 (28)
          Match:  dscp af33 (30)
          Queueing
          queue limit 1041 packets
          (queue depth/total drops/no-buffer drops) 0/0/0
          (pkts output/bytes output) 0/0
          bandwidth remaining ratio 4
        Class-map: TS_LOW_QUEUE (match-any)
          0 packets, 0 bytes
          5 minute offered rate 0000 bps
          Match:  dscp default (0)
        Class-map: class-default (match-any)
          4 packets, 240 bytes
          5 minute offered rate 0000 bps, drop rate 0000 bps
          Match: any
          queue limit 1041 packets
          (queue depth/total drops/no-buffer drops) 0/0/0
          (pkts output/bytes output) 4/240
```