# IPSec in CUPS



## Revision History

| Revision Details | Release |
|---|---|
| First introduced. | 21.25 |

## Feature Description

IPSec is a suite of protocols that interact with one another to provide secure private communications across IP networks. These protocols allow the system to establish and maintain secure tunnels with peer security gateways. IPSec provides confidentiality, data integrity, access control, and data source authentication to IP datagrams.

### IPSec AH and ESP

Authentication Header (AH) and Encapsulating Security Payload (ESP) are the two main wire-level protocols used by IPSec. They authenticate (AH) and encrypt-plus-authenticate (ESP) the data flowing over that connection.

- AH is used to authenticate – but not encrypt – IP traffic. Authentication is performed by computing a cryptographic hash-based message authentication code over nearly all the fields of the IP packet (excluding those which might be modified in transit, such as TTL or the header checksum), and stores this in a newly added AH header that is sent to the other end. This AH header is injected between the original IP header and the payload.

- ESP provides encryption and optional authentication. It includes header and trailer fields to support the encryption and optional authentication. Encryption for the IP payload is supported in transport mode and for the entire packet in the tunnel mode. Authentication applies to the ESP header and the encrypted data.

# IPSec Transport and Tunnel Mode

Transport Mode provides a secure connection between two endpoints as it encapsulates IP payload, while Tunnel Mode encapsulates the entire IP packet to provide a virtual "secure hop" between two gateways.

Tunnel Mode forms the more familiar VPN functionality, where entire IP packets are encapsulated inside another and delivered to the destination. It encapsulates the full IP header and the payload.

**Note** The UP:UP ICSR over IPSec works only with Tunnel Mode. Transport Mode isn't supported.

# IPSec Terminology

## Crypto Access Control List

Access Control Lists define rules, usually permissions, for handling subscriber data packets that meet certain criteria. Crypto ACLs, however, define the criteria that must be met for a subscriber data packet to be routed over an IPSec tunnel.

Unlike other ACLs that are applied to interfaces, contexts, or one or more subscribers, crypto ACLs are matched with crypto maps. In addition, crypto ACLs contain only a single rule while other ACL types can consist of multiple rules.

Prior to routing, the system examines the properties of each subscriber data packet. If the packet properties match the criteria specified in the crypto ACL, the system initiates the IPSec policy dictated by the crypto map.

## Transform Set

Transform Sets are used to define IPSec security associations (SAs). IPSec SAs specify the IPSec protocols to use to protect packets.

Transform sets are used during Phase 2 of IPSec establishment. In this phase, the system and a peer security gateway negotiate one or more transform sets (IPSec SAs) containing the rules for protecting packets. This negotiation ensures that both peers can properly protect and process the packets.

## ISAKMP Policy

Internet Security Association Key Management Protocol (ISAKMP) policies are used to define Internet Key Exchange (IKE) SAs. The IKE SAs dictate the shared security parameters (such as which encryption parameters to use, how to authenticate the remote peer, etc.) between the system and a peer security gateway.

During Phase 1 of IPSec establishment, the system and a peer security gateway negotiate IKE SAs. These SAs are used to protect subsequent communications between the peers including the IPSec SA negotiation process.

## Crypto Map

Crypto Maps define the tunnel policies that determine how IPSec is implemented for subscriber data packets.

There are several types of crypto maps supported in CUPS. They are:

- Manual crypto maps
- IKEv2 crypto maps
- Dynamic crypto maps

## Crypto Template

A Crypto Template configures an IKEv2 IPSec policy. It includes most of the IPSec parameters and IKEv2 dynamic parameters for cryptographic and authentication algorithms. A security gateway service won't function without a configured crypto template.

Only one crypto template can be configured per service. However, a single StarOS instance can run multiple instances of the same service with each associated with that crypto template.

# DSCP Marking of ESP Packets

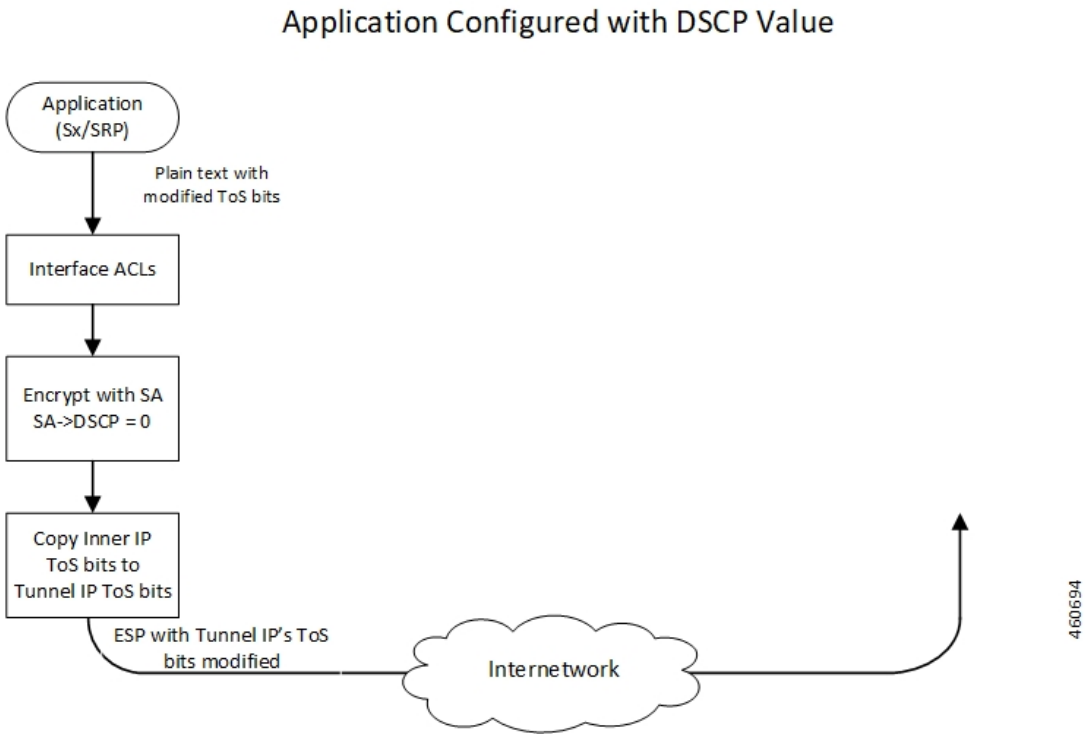
Applications such as SRP, SX, RCM, LI, and TACACS operate between nodes that are deployed across different networks. All these applications require quick turnaround while communicating with remote systems. Marking of Encapsulating Security Payload (ESP) packets with a Quality of Service (QoS) such as Differentiated Services Code Point (DSCP) helps to determine the traffic classification for these types of packets. This feature enables prioritization of IPsec packets within their IP core network, and improves scalability of interfaces such as Sx, and SRP using IPsec.

There are two ways to apply DSCP value on the ESP packets:

- Through Application configured with DSCP value
- Through Crypto Map configured with DSCP value

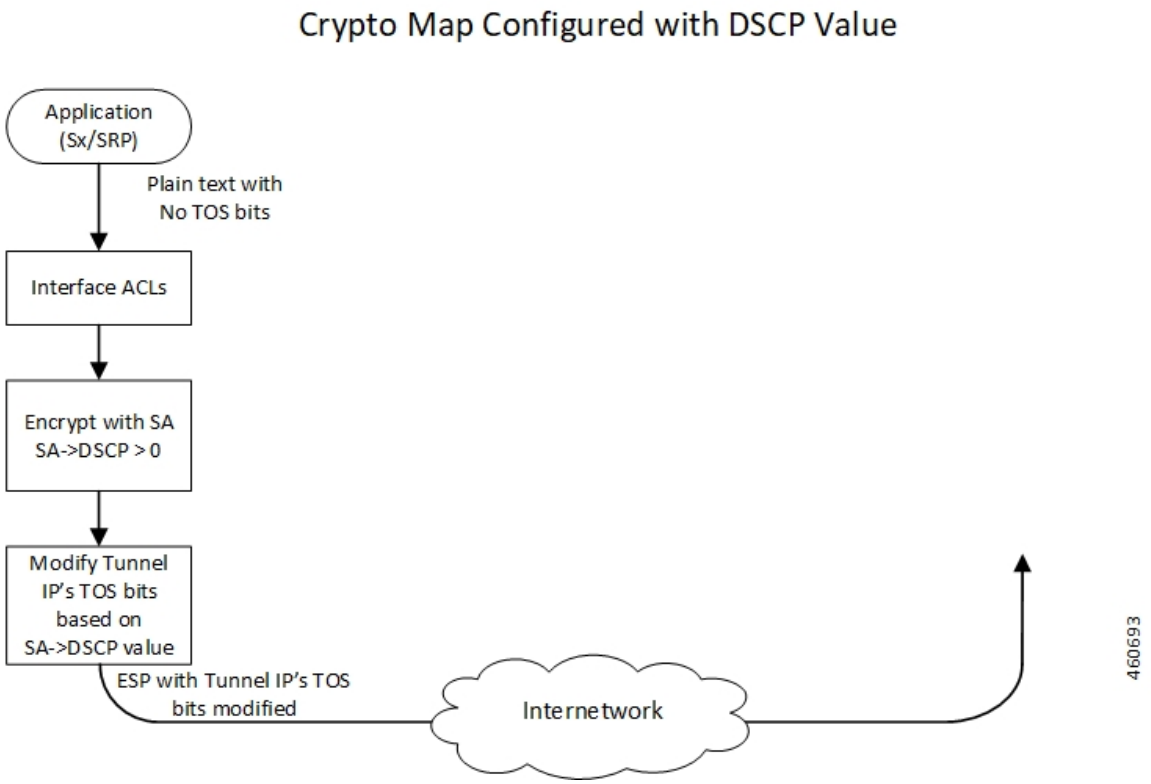
## Application Configured with DSCP Value

If an application such as SRP, SX, or LI supports DSCP configuration, the ESP packets after encryption check if the Type of Service (ToS) bits are set in the application IP header. If the ToS bits of the application IP header are non-zero, it copies the inner ToS bits to the ToS bits of tunnel IP header, and egress the packet. The following figure illustrates the operating procedure.



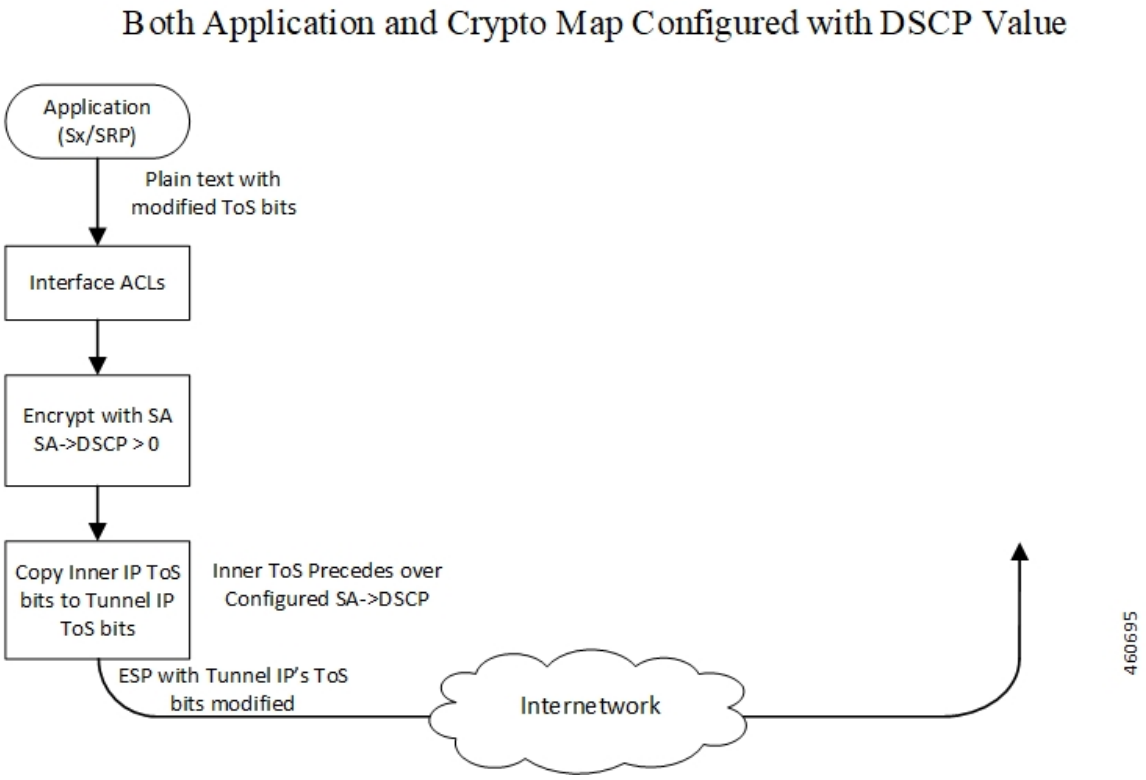

## Crypto Map Configured with DSCP Value

Every application that needs to be encrypted has an associated crypto map, which is user configurable. Once the crypto map is enabled on the specific interface, Security Association (SA) database for this crypto map is updated with a DSCP value. A new field is defined in the SA database structure to hold the DSCP value. Once the packet is encrypted, it checks if the SA database has a valid DSCP value. If a valid DSCP value is found, then this DSCP value is copied to the ToS bits of tunnel IP header, and the packet is egressed. The following figure illustrates the operating procedure.




## Application and Crypto Map Configured with DSCP Value

If the DSCP value is configured in both crypto map and application IP header, the application ToS bits take precedence, and this value is copied to the ToS bits of Tunnel IP header. The following figure illustrates the operating procedure.




# Supported Algorithms

IPSec in CUPS supports the protocols in the table below, which are specified in RFC 5996.

| Protocol | Type | Supported Options (without VPP) | Supported Options (with VPP) |
|---|---|---|---|
| Internet Key | IKEv2 Encryption | DES-CBC, 3DES-CBC, AES-CBC-128, AES-CBC-256 | |
| Exchange version 2 | IKEv2 Pseudo Random Function | PRF-HMAC-SHA1, PRF-HMAC-MD5, AES-XCBC-PRF-128 | PRF-HMAC-SHA1, PRF-HMAC-MD5, AES-XCBC-PRF-128 |
| | IKEv2 Integrity | HMAC-SHA1-96, HMAC-SHA2-256-128, HMAC-SHA2-384-192. HMAC-SHA2-512-256, HMAC-MD5-96, AES-XCBC-96 | HMAC-SHA1-96, HMAC-SHA2-256-128, HMAC-SHA2-384-192. HMAC-SHA2-512-256, HMAC-MD5-96, AES-XCBC-96 |
| | IKEv2 Diffie-Hellman Group | Group 1 (768-bit), Group 2 (1024-bit), Group 5 (1536-bit), Group 14 (2048-bit) | Group 1 (768-bit), Group 2 (1024-bit), Group 5 (1536-bit), Group 14 (2048-bit) |

| Protocol | Type | Supported Options (without VPP) | Supported Options (with VPP) |
|---|---|---|---|
| IP Security | IPSec Encapsulating Security Payload Encryption | NULL, DES-CBC, 3DES-CBC, AES-CBC-128, AES-CBC-256, AES-128-GCM-128, AES-128-GCM-64, AES-128-GCM-96, AES-256-GCM-128, AES-256-GCM-64, AES-256-GCM-96 | NULL, DES-CBC, 3DES-CBC, AES-CBC-192, AES-CBC-128, AES-CBC-256, AES-128-GCM-128, AES-128-GCM-64, AES-128-GCM-96, AES-192-GCM, AES-256-GCM-128, AES-256-GCM-64, AES-256-GCM-96 |
| | Extended Sequence Number | Value of 0 or off is supported (ESN itself is not supported) | Value of 0 or off is supported (ESN itself is not supported) |
| | IPSec Integrity | NULL, HMAC-SHA1-96, HMAC-MD5-96, AES-XCBC-96, HMAC-SHA2-256-128, HMAC-SHA2-384-192, HMAC-SHA2-512-256<br>**Important** HMAC-SHA2-384-192 and HMAC-SHA2-512-256 are not supported on VPC-DI and VPC-SI platforms if the hardware doesn't have crypto hardware. | NULL, HMAC-SHA1-96, HMAC-MD5-96, HMAC-SHA2-256-128, HMAC-SHA2-384-192, HMAC-SHA2-512-256<br>**Important** HMAC-SHA2-384-192 and HMAC-SHA2-512-256 are not supported on VPC-DI and VPC-SI platforms if the hardware doesn't have crypto hardware. |

**Note** For more information about IPSec, refer the StarOS *IPSec Reference*. Note that not all features/functionality are applicable for CUPS.

For detailed information about IPSec for Sx, LI, SRP, and so on, refer the relevant chapters in the CUPS CP Guide, CUPS UP Guide, Sx Interface Guide, and CUPS LI Guide.

# Limitations and Restrictions

Following are the limitations and restrictions for this feature:

- The feature doesn't support modification of application ToS.
- DSCP value configuration in the crypto map CLI command must be added in the same context where the application is configured as **Day-1** configuration on the UP.
- If the DSCP configuration is applied after the tunnel is created, the associated crypto maps must be re-applied on the interfaces.
- If reordering of packets occurs in an SA, the receiver might discard packets because of anti-replay mechanism.

# Configuring DSCP in Crypto Map

Use the following CLI commands to apply the DSCP value for the specific transform set.

```
configure
    context context_name
      ipsec transform-set set_name
        dscp dscp_value
        exit
      exit
    end
```

# Sample Configuration

The following is a sample configuration:

```
context ipsec-d
    ip access-list foo0
      permit tcp 209.165.200.225 209.165.200.250 209.165.200.245 209.165.200.250

    #exit

    ip access-list foo1
      permit tcp 209.165.200.225 209.165.200.250 209.165.200.247 209.165.200.250
    #exit
    ipsec transform-set A-foo
    dscp 0x28
    #exit
    ikev2-ikesa transform-set ikesa-foo
    #exit
crypto map foo0 ikev2-ipv4
      match address foo0
      authentication local pre-shared-key encrypted key encrypted_key
      authentication remote pre-shared-key encrypted key encrypted_key
      ikev2-ikesa max-retransmission 3

      ikev2-ikesa retransmission-timeout 15000

      ikev2-ikesa setup-timer 60

      ikev2-ikesa transform-set list ikesa-foo

      ikev2-ikesa rekey

      payload foo-sa0 match ipv4
        ipsec transform-set list A-foo
        lifetime 9000
        rekey keepalive
      #exit
      peer 209.165.201.1

      ikev2-ikesa policy error-notification

    #exit
    crypto map foo1 ikev2-ipv4

      match address foo1
```

```
    authentication local pre-shared-key encrypted key encrypted_key
    authentication remote pre-shared-key encrypted key encrypted_key
    ikev2-ikesa max-retransmission 3

    ikev2-ikesa retransmission-timeout 15000

    ikev2-ikesa transform-set list ikesa-foo

    ikev2-ikesa rekey

    payload foo-sa0 match ipv4

      ipsec transform-set list A-foo

      lifetime 9000

      rekey keepalive

    #exit

    peer 209.165.201.2

    ikev2-ikesa policy error-notification

  #exit
```

# Configuring QoS

The ESP packets that are marked with DSCP follow the underlying L2 marking infrastructure.

The configuration to set up QoS based on the DSCP triggers the L2 marking of the ESP packets before egress from the chassis.

The following is a sample configuration:

```
Config
  qos ip-dscp-iphb-mapping dscp 0x28 internal-priority cos 0x1
  qos l2-mapping-table name l2Marktable
     internal-priority cos 0x1 color 0x0 802.1p-value 0x4 mpls-tc 0x6
   exit
end
```

**NOTES**:

- **qos ip-dscp-iphb-mapping**: Creates a QOS profile.
- **dscp** *dscp_value*: Maps the IP DSCP values to the internal QoS.
- **internal-priority cos** *class_of_service_value* **color** *color_value* **802.1p-value** *mpls_tc_value*: Maps internal QoS priority with COS values.

The following is a sample configuration to associate L2 mapping table in IPsec context:

```
config
    context ipsec-s
       associate l2-mapping-table name l2Marktable
end
```

**NOTES**:

- **associate l2-mapping-table**: Maps QoS from internal QoS to l2 values.
- **name** *table_name*: Specifies the name of table to map QoS from internal QoS to l2 values. *table_name* must be an alphanumeric string of size 1–80.

# Monitoring and Troubleshooting

This section describes the CLI commands available to monitor and/or troubleshoot the DSCP Marking of ESP Packets feature.

## Show Commands and Outputs

This section provides information regarding show commands and their outputs in support of this feature.

**show crypto map tag** *tag_name*: Use this command to display the configured DSCP value.

```
Map Name: foo0
=======================================

  IPSec Manager: 54
  Map status: Complete
  Payload:
 ACLs:
   foo0
 Rules:
   permit tcp 209.165.200.225 209.165.200.250 209.165.200.245 209.165.200.250 eq 6002
  Crypto Map Type: IPSEC IKEv2 over IPv4
  IKE SA Transform 1/1
    Transform Set:
      Encryption Cipher: aes-cbc-128
      Encryption Accel: None
      Pseudo Random Function: sha1
      Hashed Message Authentication Code: sha1-96
      HMAC Accel: None
      Diffie-Hellman Group: 2
  IKE SA DSCP Value:  0x28

  IKE SA IDi [Peer]: Disabled

  IKE SA DH Exponentials reuse groups : None

  IKEv2 IKESA DDOS Mitigation Params:
    Half Open Timer: Disabled
    Decrypt Fail Count: Disabled
    Max IKEv2 requests Allowed : Disabled
    Message Queue Size: Disabled
    Rekey Rate: Disabled
    Max Certificate Size: Disabled

  IKEv2 Notify Payload:
    Device Identity: Enabled[Default]
  Notify Payload Error Message Type:
    UE: 0
    Network Transient Minor: 0
    Network Transient Major: 0
    Network Permanent: 0
```

```
Blacklist/Whitelist : None

OCSP Status         : Disabled
OCSP Nonce Status  : Enabled
OCSP Responder Address :None
OCSP HTTP version : 1.0


Remote-secret-list: <not-configured>

Authentication Local:
 Phase 1 - Pre-Shared Key (Size = 7)

Authentication Remote:
 Phase 1 - Pre-Shared Key (Size = 7)


Self-Certificate Validation: Disabled
Certificate Server Timeout: 20 Sec
Minimum Certificate Key Size Validation: Disabled


Max Dhost Connections: 40

IPSec SA Payload 1/1
  Name : foo-sa0
  Payload Maximum Child SA: 1 [Default]
  Payload Ignore Ikesa Rekey: Disabled
  Payload Lifetime Params:
    Seconds: 90
    Sequence Number: 4293918720 [Default]
  Payload TSI Start Address: Address Endpoint
  Payload TSI End Address: Address Endpoint

  IPSec SA Transform 1/1
    Transform Set:
      Protocol: esp
      Encryption Cipher: aes-cbc-128
      Encryption Accel: None
      Hashed Message Authentication Code: sha1-96
      HMAC Accel: None
      Diffie-Hellman Group: none
      ESN: Disabled
      Dscp: 0x28
Dont Fragment: Copy bit from inner header
IPv4 Payload fragment type: outer
MTU: 1438 [Default]

NATT: Disabled


IKEv2 Fragmentation: Enabled
IKEv2 MTU Size IPv4/IPv6: 1384/1364

CERT Enc Type URL Allowed: Disabled
Custom FQDN Allowed: Disabled
DNS Handling: Normal [Default]

interface using this crypto-map: saegw-li1-loopback-ipv4

Local Gateway: 209.165.202.129
Remote Gateway: 209.165.201.1
```

**show qos ip-dscp-iphb-mapping**: Use this command to display mapping QoS information in a packet to internal-qos marking.

| DSCP | Internal Qos |
|---|---|
| 0x00 | 0 |
| 0x01 | 0 |
| 0x02 | 0 |
| 0x03 | 0 |
| 0x04 | 0 |
| 0x05 | 0 |
| 0x06 | 0 |
| 0x07 | 0 |
| 0x08 | 0 |
| 0x09 | 0 |
| 0x0a | 0 |
| 0x0b | 0 |
| 0x0c | 0 |
| 0x0d | 0 |
| 0x0e | 0 |
| 0x0f | 0 |
| 0x10 | 0 |
| 0x11 | 0 |
| 0x12 | 0 |
| 0x13 | 0 |
| 0x14 | 0 |
| 0x15 | 0 |
| 0x16 | 0 |
| 0x17 | 0 |
| 0x18 | 0 |
| 0x19 | 0 |
| 0x1a | 0 |
| 0x1b | 0 |
| 0x1c | 0 |
| 0x1d | 0 |
| 0x1e | 0 |
| 0x1f | 0 |
| 0x20 | 0 |
| 0x21 | 0 |
| 0x22 | 0 |
| 0x23 | 0 |
| 0x24 | 0 |
| 0x25 | 0 |
| 0x26 | 0 |
| 0x27 | 0 |
| **0x28** | **1** |
| 0x29 | 0 |
| 0x2a | 0 |
| 0x2b | 0 |
| 0x2c | 0 |
| 0x2d | 0 |
| 0x2e | 0 |
| 0x2f | 0 |
| 0x30 | 0 |
| 0x31 | 0 |
| 0x32 | 0 |
| 0x33 | 0 |

```
   0x34       |          0
   0x35       |          0
   0x36       |          0
   0x37       |          0
--------------+-----------------
   0x38       |          0
   0x39       |          0
   0x3a       |          0
   0x3b       |          0
   0x3c       |          0
   0x3d       |          0
   0x3e       |          0
   0x3f       |          0
--------------+-----------------
```

**show qos l2-mapping-table name** *table_name* : Use this command to display named table for the internal to L2 mapping values.

```
Table: l2Marktable
------------------------+-------+-------
    Internal Priority    |802.1p | MPLS
 Class-of-service | Color|       |
------------------+------+-------+-------
       0          |   0  | 0x0   |    0
       0          |   1  | 0x0   |    0
       0          |   2  | 0x0   |    0
       0          |   3  | 0x0   |    0
       1          |   0  | 0x4   |    6
       1          |   1  | 0x2   |    1
       1          |   2  | 0x2   |    1
       1          |   3  | 0x2   |    1
------------------+------+-------+-------
       2          |   0  | 0x4   |    2
       2          |   1  | 0x4   |    2
       2          |   2  | 0x4   |    2
       2          |   3  | 0x4   |    2
       3          |   0  | 0x6   |    3
       3          |   1  | 0x6   |    3
       3          |   2  | 0x6   |    3
       3          |   3  | 0x6   |    3
------------------+------+-------+-------
       4          |   0  | 0x8   |    4
       4          |   1  | 0x8   |    4
       4          |   2  | 0x8   |    4
       4          |   3  | 0x8   |    4
       5          |   0  | 0xa   |    5
       5          |   1  | 0xa   |    5
       5          |   2  | 0xa   |    5
       5          |   3  | 0xa   |    5
------------------+------+-------+-------
       6          |   0  | 0xc   |    6
       6          |   1  | 0xc   |    6
       6          |   2  | 0xc   |    6
       6          |   3  | 0xc   |    6
       7          |   0  | 0xe   |    7
       7          |   1  | 0xe   |    7
       7          |   2  | 0xe   |    7
       7          |   3  | 0xe   |    7
------------------+------+-------+-------
```