Chapter 38

Generic Packet Classifier

Introduction

The classifier enables you to create packet matching rules—called *classifiers*—to sort packets into *data flows*. For example, you may want all packets with the same destination TCP/IP port to form a flow (e.g. all telnet or HTTP traffic). This chapter describes how to configure the classifier.

You can then configure the router to process all packets in a data flow in a given manner, through Quality of Service (QoS). QoS prioritises packets and manages bandwidth. QoS is particularly useful for improving VoIP and video links, especially if your network is congested. Theory and configuration of QoS is described in Chapter 39, Software Quality of Service (QoS).

Configuration of Classifiers

Configuring the classifier involves creating a set of packet matching rules, called *classifiers*, using the command:

```
create classifier=1..9999 [options]
```

These classifiers can identify any single packet based upon many criteria. Available criteria depend on the type of interface you use the classifier on, and include:

- Physical (layer 1) and layer 2 port or interface

  You can classify packets according to their ingress or egress port or ingress interface, and VLAN settings.

- Ethernet encapsulation type

  You can classify packets depending on the specific protocol type of each frame. Different values indicate how the packet is formatted. For example, a value of 802.2 indicates the packet is formatted according to IEEE standards 802.2 and 802.3 with a Destination Service Access Point/Source Service Access Point (DSAP/SSAP) value not equal to AAAA in hexadecimal; SAP encapsulation. A value of ETHII indicates the packet is formatted according to RFC 894; Ethernet II encapsulation. For more details on values see the ETHFORMAT parameter in the **create classifier** command on page 38-4.

- Source/Destination MAC address

  You can classify frames from a specific source or destination MAC address. This classification can be used for users on remote networks. You can also specify MAC type to distinguish unicast packets from broadcast or multicast packets.

- Frame relay, ATM and PPP settings

  You can classify according to DLCI, PPP index number or PPP protocol ID, and ATM VCI or VPI.

- Layer 3 protocols

  You can classify frames based on any value for Layer 3 protocols. Layer 3 protocol and Ethernet encapsulation types are interrelated, e.g. IPX Ethernet II encapsulated packets are different to IPX NETWARERAW encapsulated packets.

- DiffServ or IP TOS

  You can classify packets according to the value of the DSCP bits in the DiffServ field of the header, or the TOS precedence bits in the Type of Service (TOS). These fields are alternatives, so are mutually exclusive.

- Source/destination IP or IPv6 address and other IP settings

  You can classify packets based on an exact match of the source or destination IP address information within the IP or IPv6 header, and based on the presence of several other header fields.

- Layer 4 protocol (TCP/UDP, ICMP etc.)

  You can classify packets based on specific Layer 4 TCP or UDP destination and source port numbers contained within the IP or IPv6 header.

- Layer 4 source/destination port and other layer 4 settings

  You can classify packets based on a specific port number or a range of port numbers, and based on TCP flags, ICMP code and ICMP type.

Command Reference

This section describes the commands available to configure and manage the classifiers.

See "Conventions" on page lxv of About this Software Reference in the front of this manual for details of the conventions used to describe command syntax. See Appendix A, Messages for a complete list of messages and their meanings.

create classifier

Classifier parameters are sorted approximately in order of the OSI model, with layer 1 (physical) parameters first.

Syntax: software QoS on ingress

For classifiers to use with software QoS on ingress traffic over ETH ports; frame relay, ATM, and PPP interfaces; and the switch ports as a single instance:

```
CREate CLASSifier=1..9999
   [IPDScp={dscp-list|ANY}] [IPTOs={0..7|ANY}]
   [VLANPriority={priority-list|ANY}]
```

Syntax: software QoS on egress

For classifiers to use with software QoS on egress traffic over ETH ports; frame relay, ATM, and PPP interfaces; and the switch ports as a single instance:

```
CREate CLASSifier=1..9999 [IINTerface={interface|NONE}]
   [EPOrt={port|ANY}] [IPOrt={port|ANY}]
   [SVlan={vlan-name|1..4094|ANY}]
   [DVlan={vlan-name|1..4094|ANY}]
   [VLANPriority={priority-list|ANY}]
   [ETHFormat={802.2|802.2-Tagged|802.2-Untagged|Ethii|
   ETHII-Tagged|ETHII-Untagged|Netwareraw|
   NETWARERAW-Tagged|NETWARERAW-Untagged|Snap|SNAP-Tagged|
   SNAP-Untagged|ANY}]
   [MACDaddr={macadd|ANY}] [MACSaddr={macadd|ANY}]
   [MACType={L2Ucast|L2BMcast|ANY}]
   [ATMVCI={vci-list|ANY}] [ATMVPI={vpi-list|ANY}]
   [DLCi={dlci-range|ANY}] [PPPIndex=0..1023]
   [PPPProtocolid={ppp-protocol-id|IP|IPv6|ANY}]
   [PROTocol={protocol-type|ARP|IP|IPV6|IPX|ANY}]
   [IPDAddr={ipadd[/0..32]|ipv6add[/0..128]|ANY}]
   [IPSAddr={ipadd[/0..32]|ipv6add[/0..128]|ANY}]
   [IPDScp={dscp-list|ANY}] [IPTOs={0..7|ANY}]
   [IPFRAg={YES|NO|ANY}] [IPOPtions={YES|NO|ANY}]
   [IPFLowlabel={0..1048575|ANY}]
   [IPPRotocol={TCP|UDP|ICMp|IGMp|OSPf|NONTcpudp|ANY|
   ip-protocol}]
   [ICmptype={Any|ECHORply|Unreachable|Quench|Redirect|
   ECHO|ADvertisement|Solicitation|TImeexceed|Parameter|
   TSTAMP|TSTAMPRply|INFOREQ|INFOREP|ADDRREQ|ADDRREP|
   NAMEREq|NAMERPly|icmp-type}]
   [ICMPCode={Any|FIlter|FRAGMent|FRAGReassm|HOSTComm|
   HOSTIsolated|HOSTPrec|HOSTREdirect|HOSTRTos|HOSTTos|
   HOSTUNKnown|HOSTUNReach|NETComm|NETREdirect|NETRTos|
   NETTos|NETUNKnown|NETUNReach|NOptr|POrtunreach|
   PREcedent|PROtunreach|PTrproblem|Sourceroute|Ttl|
   icmp-code}]
   [TCPFlags={{Urg|Ack|Rst|Syn|Fin}[,...]|ANY}]
   [TCPDport={port-range|ANY}] [TCPSport={port-range|ANY}]
   [UDPDport={port-range|ANY}] [UDPSport={port-range|ANY}]
```

Syntax: software QoS on tunnels

For classifiers to use with software QoS on GRE, IPsec and 6-to-4 tunnels:

```
CREate CLASSifier=1..9999 [IINTerface={interface|NONE}]
   [IPDAddr={ipadd[/0..32]|ipv6add[/0..128]|ANY}]
   [IPSAddr={ipadd[/0..32]|ipv6add[/0..128]|ANY}]
   [IPDScp={dscp-list|ANY}] [IPTOs={0..7|ANY}]
   [IPFRAg={YES|NO|ANY}] [IPOPtions={YES|NO|ANY}]
   [IPFLowlabel={flow-label-range|ANY}]
   [IPPRotocol={TCP|UDP|ICMp|IGMp|OSPf|NONTcpudp|ANY|
   ip-protocol}]
   [ICmptype={Any|ECHORply|Unreachable|Quench|Redirect|
   ECHO|ADvertisement|Solicitation|TImeexceed|Parameter|
   TSTAMP|TSTAMPRply|INFOREQ|INFOREP|ADDRREQ|ADDRREP|
   NAMEREq|NAMERPly|icmp-type}]
   [ICMPCode={Any|FIlter|FRAGMent|FRAGReassm|HOSTComm|
   HOSTIsolated|HOSTPrec|HOSTREdirect|HOSTRTos|HOSTTos|
   HOSTUNKnown|HOSTUNReach|NETComm|NETREdirect|NETRTos|
   NETTos|NETUNKnown|NETUNReach|NOptr|POrtunreach|
   PREcedent|PROtunreach|PTrproblem|Sourceroute|Ttl|
   icmp-code}]
   [TCPFlags={{Urg|Ack|Rst|Syn|Fin}[,...]|ANY}]
   [TCPDport={port-range|ANY}] [TCPSport={port-range|ANY}]
   [UDPDport={port-range|ANY}] [UDPSport={port-range|ANY}]
```

Description

This command creates a classifier, to sort traffic into flows. Classifiers are packet matching rules that identify particular data flows. The data flows may be specific in nature (e.g. IP packets with a particular TCP destination port from a particular source IP address) or general (e.g. all ICMP packets).

You can use up to 64 classifiers per software QoS policy. Both static classifiers and the dynamic classifiers created by DAR objects count towards this limit.

Parameter	Description
CLASSifier	The ID number of the new classifier. An integer in the range 1 to 9999. The software QoS traffic class ID number and classifier ID number together determine the rule matching order. Classifiers within each traffic class are checked in ascending order of ID number (lowest first). Default: no default
Layer 1 parameters	
EPOrt	The egress port—the Ethernet switch port through which the frame is destined to leave the router. An integer in the range 1 to *n*, where *n* is the highest switch port. Default: **any** (ignores egress port)
IPOrt	The ingress port—the Ethernet switch port through which the frame arrives at the router. An integer in the range 1 to *n*, where *n* is the highest switch port. **Iport** and **iinterface** are mutually exclusive. Default: **any** (ignores ingress port)

Parameter (cont.)	**Description** (cont.)
IINTerface	The ingress interface—the interface through which the frame arrives at the router. Valid entries are Layer 1 and 2 interfaces: ● eth (such as. eth0) ● ATM channel (such as atm0.0) ● frame relay (e.g. fr0) ● PPP (such as ppp0) To see a list of current valid Layer 1 and 2 interfaces, use the **show interface** command on page 9-72 of Chapter 9, Interfaces. **Iport** and **iinterface** are mutually exclusive. **Iinterface** is only valid in classifiers for software QoS on egress interfaces or tunnels. Default: **none** (ignores ingress interface)

Layer 2 Ethernet parameters

SVlan	The source VLAN—the VLAN associated with the frame when it arrives at the router. Only valid in classifiers for software QoS on egress interfaces. Default: **any**	
	vlan-name	The name of the source VLAN. To see a list of current VLANs, use the **show vlan** command on page 8-54 of Chapter 8, Switching.
	1..4094	The VLAN Identifier (VID) of the source VLAN.
	ANY	The classifier ignores the source VLAN.
DVlan	The destination VLAN—the VLAN that the frame will be transmitted to. Only valid in classifiers for software QoS on egress interfaces. Default: **any**	
	vlan-name	The name of the destination VLAN. To see a list of current VLANs, use the **show vlan** command on page 8-54 of Chapter 8, Switching.
	1..4094	The VLAN Identifier (VID) of the destination VLAN.
	ANY	The classifier ignores the destination VLAN.
VLANPriority	The 802.1p VLAN priority value in the frame. An integer in the range 0 to 7; a range of integers separated by hyphens; or a comma separated list of integers and/or ranges (for example 0,2,4-6). Only valid in classifiers for software QoS on ingress and egress interfaces. Default: **any** (ignores VLAN priority)	

Layer 2 Ethernet parameters (cont.)		
ETHFormat	The Ethernet encapsulation type of the frame. The **ethformat** and **protocol** must match. Table 38-1 on page 38-11 shows possible combinations and whether they are valid. You can distinguish between frames that are tagged and untagged at ingress. Default: **any**	
	802.2 802.2-Tagged 802.2-Untagged	Formatted according to IEEE Standards 802.2 and 802.3 with a DSAP/SSAP value not equal to hexadecimal AAAA. Encapsulation: SAP
	Ethii ETHII-Tagged ETHII-Untagged	Formatted according to RFC 894, *Standard for the transmission of IP datagrams over Ethernet networks.* Encapsulation: Ethernet II
	Netwareraw NETWARERAW-Tagged NETWARERAW-Untagged	Formatted as an IPX packet according to IEEE Standard 802.3. Encapsulation: NetWare Raw or Novell
	Snap SNAP-Tagged SNAP-Untagged	Formatted according to IEEE Standards 802.2 and 802.3 and RFC 1042, *Standard for the transmission of IP datagrams over IEEE 802 networks.* Encapsulation: SNAP
	ANY	The classifier ignores the Ethernet encapsulation.
MACDaddr	The destination MAC address of the frame. An Ethernet six-octet MAC address, expressed as six pairs of hexadecimal digits delimited by hyphens. Default: **any** (ignores destination MAC address).	
MACSaddr	The source MAC address of the frame. An Ethernet six-octet MAC address, expressed as six pairs of hexadecimal digits delimited by hyphens. Default: **any** (ignores source MAC address).	
MACType	The type of destination MAC address on the frame. Only valid in classifiers for software QoS on egress interfaces. Default: **any**	
	L2Ucast	Layer 2 unicast addresses.
	L2BMcast	Layer 2 broadcast or multicast addresses.
	ANY	The classifier ignores the MAC address type.

Layer 2 Ethernet parameters (cont.)

PROTocol — The protocol, determined from the value of the following Ethernet field:

- for 802.2 (SAP encapsulation): the DSAP field, 1 byte hexadecimal
- for ETHII encapsulation: the ETYPE field, 2 bytes hexadecimal
- for NETWARERAW encapsulation: the IPX checksum field, 2 bytes hexadecimal with value FFFF
- for SNAP encapsulation: the ETYPE field, 5 bytes hexadecimal. The classifier matches on the last 2 bytes.

The encapsulation type (**ethformat** parameter) and **protocol** must match. Table 38-1 on page 38-11 shows possible combinations and whether they are valid.

Default: **any**, unless you also specify a TCP or UDP parameter (for example, **tcpsport**). Then the default is **IP**.

protocol-type	The protocol number or the predefined protocol name. Table 38-2 on page 38-13 shows predefined protocols, their numbers, and their encapsulations.
IP	Internet Protocol version 4. Valid with **ethformat** of **ethii** or **snap**.
IPV6	Internet Protocol version 6. Valid with **ethformat** of **ethii**.
ARP	Address Resolution Protocol. Valid with **ethformat** of **ethii** or **snap**.
IPX	IPX. Valid with **ethformat** of **802.2**, **ethii**, **netwareraw** or **snap**.
ANY	The classifier ignores the protocol.

Layer 2 parameters (ATM, frame relay and PPP)

ATMVCi — The Virtual Channel Identifier for an ATM connection. An integer in the range 0 to 255, or a range of integers separated by a hyphen (for example 0-3). Only valid in classifiers for software QoS on egress interfaces.

Default: **any** (ignores ATM VCI).

ATMVPi — The Virtual Path Identifier for an ATM connection. An integer in the range 0 to 4095, or a range of integers separated by a hyphen (for example 0-3). Only valid in classifiers for software QoS on egress interfaces.

Default: **any** (ignores ATM VPI).

DLCi — The identification number of a Frame Relay Data Link Connection (DLC). An integer in the range 0 to 1023, or a range of integers separated by a hyphen (for example 0-3). Only valid in classifiers for software QoS on egress interfaces.

Default: **any** (ignores DLCI).

PPPIndex — The PPP interface number. For example, for ppp2, **pppindex**=**2**.

Layer 2 parameters (ATM, frame relay and PPP) (cont.)

PPPProtocolid	The network layer protocol of the PPP encapsulated packet. Note that network and link control packets are processed by the software QoS policy's system traffic class. Examples of control packets include NCP, LCP, IPCP and PAP. Only valid in classifiers for software QoS on egress interfaces. Default: **any**, unless you also specify a TCP or UDP parameter. Then the default is **IP**.	
	ppp-protocol-id|	A 4 byte hexadecimal protocol number. Table 38-3 on page 38-14 shows valid protocols and numbers.
	IP	Internet Protocol.
	IPV6	Internet Protocol version 6.
	ANY	The classifier ignores PPP protocol ID.

Layer 3 parameters

IPDAddr	The destination IPv4 or IPv6 address of the packet. Default: **any**	
	ipadd[/0..32]	The destination IPv4 address, in dotted decimal notation. You can optionally specify a subnet by specifying a mask.
	ipv6add[/0..128]	The destination IPv6 address, specified as eight pairs of hexadecimal octets separated by colons. You can optionally specify a prefix length. Default prefix length is 128—a single address. IPv6 addresses are only valid in classifiers for software QoS on egress or tunnel interfaces.
	ANY	The classifier ignores destination IP or IPv6 address.
IPSAddr	The source IPv4 or IPv6 address of the packet. Default: **any**	
	ipadd[/0..32]	The source IPv4 address, in dotted decimal notation. You can optionally specify a subnet by specifying a mask.
	ipv6add[/0..128]	The source IPv6 address, specified as eight pairs of hexadecimal octets separated by colons. You can optionally specify a prefix length. Default prefix length is 128—a single address. IPv6 addresses are only valid in classifiers for software QoS on egress or tunnel interfaces.
	ANY	The classifier ignores source IPv4 or IPv6 address.
IPDScp	The DSCP value—the Code Point bits of the DiffServ field of an IPv4 or IPv6 packet. An integer in the range 0 to 63; a range of integers separated by hyphens; or a comma separated list of integers and/or ranges (for example 0,2,4-6). You can also specify EF, AF1, AF2, AF3 or AF4. **Ipdscp** and **Iptos** are mutually exclusive. Default: **any** (ignores DSCP).	
IPTOs	The TOS value—the value of the precedence field within the TOS byte of an IPv4 packet. An integer in the range 0 to 7. **Ipdscp** and **Iptos** are mutually exclusive. **Iptos** is only valid for IPv4 packets. Default: **any** (ignores TOS).	

Layer 3 parameters (cont.)	
IPFRAg	Whether the IPv4 packet is fragmented. Only valid in classifiers for software QoS on egress or tunnel interfaces. Default: **any** (ignores whether the packet is fragmented).
IPOPtions	Whether the packet includes the IPv4 header options field. Only valid in classifiers for software QoS on egress or tunnel interfaces. Default: **any** (ignores whether the header options field is present or not).
IPFLowlabel	The IPv6 flow label in an IPv6 packet, an integer in the range 0 to 1048575. Only valid for IPv6 packets in classifiers for software QoS on egress or tunnel interfaces. Default: **any** (ignores IPv6 flow label).
IPPRotocol	The Layer 4 IPv4 or IPv6 protocol of the packet. For IPv6 packets, **ipprotocol** matches against the Next Header field of the IPv6 packet header. You can use a total of 29 unique **ipprotocol** values, plus TCP and UDP, in total across all classifiers. Default: ● **tcp** if you also specify a TCP parameter (for example, **tcpsport**). ● **udp** if you also specify a UDP parameter (for example, **udpsport**). ● Otherwise, **any** (ignores IP protocol).

ip-protocol	A 1 byte decimal IPv4 or IPv6 protocol number or a well-known protocol name.
TCP	Transmission Control Protocol.
UDP	User Datagram Protocol.
NONTcpudp	Any IPv4 or IPv6 protocol except TCP or UDP.
ICMp	Internet Control Message Protocol.
IGMp	Internet Group Multicast Protocol.
OSPf	Open Shortest Path First.
ANY	The classifier ignores the IP protocol value.

Layer 4 parameters	
ICmptype	The ICMP message type to match against the ICMP type field in an ICMP packet header. One of the list of options, or a decimal value in the range 0 to 65535. Only valid if **ipprotocol=icmp** in classifiers for software QoS on egress or tunnel interfaces. Default: **any** (ignores ICMP type).
ICMPCode	The ICMP message reason code to match against the ICMP code field in an ICMP packet header. One of the list of options, or a decimal value in the range 0 to 65535. Only valid if **ipprotocol=icmp** in classifiers for software QoS on egress or tunnel interfaces. Default: **any** (ignores ICMP code).
TCPFlags	The TCP flags of the TCP/IP packet. One or a comma-separated list of the options URG, ACK, RST, SYN and FIN. Default: **any** (ignores TCP flag).
TCPDport	The destination TCP port—the value in the TCP destination port field of the packet. For classifiers for software QoS on egress or tunnel interfaces, a single port number or a range of port numbers separated by a hyphen. Default: **any** (ignores destination TCP port).

Layer 4 parameters (cont.)	
TCPSport	The source TCP port—the value in the TCP source port field of the packet. For classifiers for software QoS on egress or tunnel interfaces, a single port number or a range of port numbers separated by a hyphen. Default: **any** (ignores source TCP port).
UDPDport	The destination UDP port—the value in the UDP destination port field of the packet.For classifiers for software QoS on egress or tunnel interfaces, a single port number or a range of port numbers separated by a hyphen. Default: **any** (ignores destination UDP port).
UDPSport	The source UDP port—the value in the UDP source port field of the packet. For classifiers for software QoS on egress or tunnel interfaces, a single port number or a range of port numbers separated by a hyphen. Default: **any** (ignores source UDP port).

Table 38-1: Possible **ethformat** and **protocol** parameter combinations

ethformat	**protocol**	**validity**
ETHII	[not specified]	OK
	ANY	OK
	ARP	OK
	IP	OK (equivalent to protocol=0800)
	IPV6	OK
	IPX	OK (equivalent to protocol=8137)
	protocol-type	OK (see Table 38-2 for valid combinations)
NETWARERAW	[not specified]	OK (equivalent to protocol="IPX 802.3")
	ANY	OK (equivalent to protocol="IPX 802.3")
	ARP	Error
	IP	Error
	IPV6	Error
	IPX	OK (equivalent to protocol="IPX 802.3")
	"IPX 802.3"	OK
	protocol-type	Error
SNAP	[not specified]	OK
	ANY	OK
	ARP	OK
	IP	OK
	IPV6	Error
	IPX	OK
	protocol-type	OK (see Table 38-2 for valid combinations)

Table 38-1: Possible **ethformat** and **protocol** parameter combinations (cont.)

ethformat	protocol	validity
802.2	[not specified]	OK
	ANY	OK
	ARP	Error
	IP	Error
	IPV6	Error
	IPX	OK
	protocol-type	OK (see Table 38-2 for valid combinations)

Table 38-2: Predefined protocol types for use in the **protocol** parameter

Protocol Name	Protocol Number	Encapsulation	Min. characters to enter
SNA Path Control	04	SAP	3
PROWAY-LAN	0E	SAP	7
EIA-RS	4E	SAP	3
PROWAY	8E	SAP	3
IPX 802.2	E0	SAP	9
NetBEUI	F0	SAP	3
ISO CLNS IS	FE	SAP	5
IP ETHII	0800	EthII	8
X.75 Internet	0801	EthII	4
NBS Internet	0802	EthII	3
ECMA Internet	0803	EthII	4
Chaosnet	0804	EthII	4
X.25 Level 3	0805	EthII	4
ARP	0806	EthII	3
XNS Compat	0807	EthII	3
Banyan Systems	0BAD	EthII	3
BBN Simnet	5208	EthII	3
DEC MOP Dump/Ld	6001	EthII	9
DEC MOP Rem Cons	6002	EthII	9
DEC DECNET	6003	EthII	7
DEC LAT	6004	EthII	7
DEC Diagnostic	6005	EthII	7
DEC Customer	6006	EthII	7
DEC LAVC	6007	EthII	7
RARP	8035	EthII	4
DEC LANBridge	8038	EthII	7
DEC Encryption	803D	EthII	7
AppleTalk	809B	EthII	3
IBM SNA	80D5	EthII	7
IPX EthII	8137	EthII	9
AppleTalk AARP	80F3	EthII	11
SNMP	814C	EthII	4
IPv6 ETHII	86DD	EthII	10
IPX 802.3	FFFF	NetWare 802.3 Raw	9
ETHERTALK 2	080007809B	SNAP	11
ETHERTALK 2 AARP	00000080F3	SNAP	13
IPX SNAP	0000008137	SNAP	8

Note: When you enter a protocol name that contains spaces, you must surround the name with double quotation marks. You can use lowercase or uppercase letters. For example, to specify ETHERTALK 2 AARP, enter **protocol="ethertalk 2 aarp"** or **protocol="ethertalk 2 a"**.

Table 38-3: PPP Network Layer protocol ID values for use in the **pppprotocolid** parameter

PPP Protocol	Number	Long Name
IP	0021	Internet Protocol
OSI	0023	OSI Network Layer
DEC	0027	Decnet Phase IV
APP	0029	Appletalk
IPX	002B	IPX
VJC	002D	Van Jacobson Compressed TCP/IP
VJU	002F	Van Jacobson Uncompressed TCP/IP
BRI	0031	Bridging PDU
MP	003D	Multilink Protocol
IP6HC	004F	IP6 Header Compression
ENC	0053	Encryption
IPV6	0057	Internet Protocol version 6
SINGLE	00FB	Single Link Compression in Multilink
Compressed	00FD	Compressed Datagram

Examples

To create packet matching rule 1 so that it matches all IP packets from the IP subnet 192.168.100.2 (mask=255.255.255.0), with a destination TCP port of 23, use one of the commands:

```
cre class=1 ipsaddr=192.168.100.2/24 tcpdport=23
```

```
cre class=1 protocol=ip ipsaddr=192.168.100.2/24 tcpdport=23
```

To create packet matching rules to separate PPPoE interfaces 1 and 2 on an Ethernet interface, use the commands:

```
cre class=1 pppi=1
```

```
cre class=2 pppi=2
```

Related Commands

destroy classifier
set classifier
show classifier

destroy classifier

Syntax `DESTroy CLASSifier={`*`rule-list`*`|ALL}`

Description This command destroys one or more packet matching rules. You cannot destroy a classifier that software QoS is using.

The **classifier** parameter specifies the classifiers to destroy, and is the rule ID of an existing classifier, a comma-separated list of rule IDs, a range of rule IDs separated by a hyphen, or a combination (for example, 3,5,9-12). If you specify **all**, then all classifiers are destroyed.

Examples To destroy the packet matching rules with rule-ids 3, 5 and 9 to 12, use the command:

```
dest class=3,5,9-12
```

To destroy all packet matching rules, use the command:

```
dest class=all
```

Related Commands

create classifier
set classifier
show classifier

set classifier

Classifier parameters are sorted approximately in order of the OSI model, with layer 1 (physical) parameters first.

Syntax: software QoS on ingress

For classifiers to use with software QoS on ingress traffic over ETH ports; frame relay, ATM, and PPP interfaces; and the switch ports as a single instance:

```
SET CLASSifier=1..9999
   [IPDScp={dscp-list|ANY}] [IPTOs={0..7|ANY}]
   [VLANPriority={priority-list|ANY}]
```

Syntax: software QoS on egress

For classifiers to use with software QoS on egress traffic over ETH ports; frame relay, ATM, and PPP interfaces; and the switch ports as a single instance:

```
SET CLASSifier=1..9999 [IINTerface={interface|NONE}]
   [EPOrt={port|ANY}] [IPOrt={port|ANY}]
   [SVlan={vlan-name|1..4094|ANY}]
   [DVlan={vlan-name|1..4094|ANY}]
   [VLANPriority={priority-list|ANY}]
   [ETHFormat={802.2|802.2-Tagged|802.2-Untagged|Ethii|
   ETHII-Tagged|ETHII-Untagged|Netwareraw|
   NETWARERAW-Tagged|NETWARERAW-Untagged|Snap|SNAP-Tagged|
   SNAP-Untagged|ANY}]
   [MACDaddr={macadd|ANY}] [MACSaddr={macadd|ANY}]
   [MACType={L2Ucast|L2BMcast|ANY}]
   [ATMVCI={vci-list|ANY}] [ATMVPI={vpi-list|ANY}]
   [DLCi={dlci-range|ANY}] [PPPIndex=0..1023]
   [PPPProtocolid={ppp-protocol-id|IP|IPv6|ANY}]
   [PROTocol={protocol-type|ARP|IP|IPV6|IPX|ANY}]
   [IPDAddr={ipadd[/0..32]|ipv6add[/0..128]|ANY}]
   [IPSAddr={ipadd[/0..32]|ipv6add[/0..128]|ANY}]
   [IPDScp={dscp-list|ANY}] [IPTOs={0..7|ANY}]
   [IPFRAg={YES|NO|ANY}] [IPOPtions={YES|NO|ANY}]
   [IPFLowlabel={0..1048575|ANY}]
   [IPPRotocol={TCP|UDP|ICMp|IGMp|OSPf|NONTcpudp|ANY|
   ip-protocol}]
   [ICmptype={Any|ECHORply|Unreachable|Quench|Redirect|
   ECHO|ADvertisement|Solicitation|TImeexceed|Parameter|
   TSTAMP|TSTAMPRply|INFOREQ|INFOREP|ADDRREQ|ADDRREP|
   NAMEREq|NAMERPly|icmp-type}]
   [ICMPCode={Any|FIlter|FRAGMent|FRAGReassm|HOSTComm|
   HOSTIsolated|HOSTPrec|HOSTREdirect|HOSTRTos|HOSTTos|
   HOSTUNKnown|HOSTUNReach|NETComm|NETREdirect|NETRTos|
   NETTos|NETUNKnown|NETUNReach|NOptr|POrtunreach|
   PREcedent|PROtunreach|PTrproblem|Sourceroute|Ttl|
   icmp-code}]
   [TCPFlags={{Urg|Ack|Rst|Syn|Fin}[,...]|ANY}]
   [TCPDport={port-range|ANY}] [TCPSport={port-range|ANY}]
   [UDPDport={port-range|ANY}] [UDPSport={port-range|ANY}]
```

Syntax: software QoS on tunnels

For classifiers to use with software QoS on GRE, IPsec and 6-to-4 tunnels:

```
SET CLASSifier=1..9999 [IINTerface={interface|NONE}]
   [IPDAddr={ipadd[/0..32]|ipv6add[/0..128]|ANY}]
   [IPSAddr={ipadd[/0..32]|ipv6add[/0..128]|ANY}]
   [IPDScp={dscp-list|ANY}] [IPTOs={0..7|ANY}]
   [IPFRAg={YES|NO|ANY}] [IPOPtions={YES|NO|ANY}]
   [IPFLowlabel={flow-label-range|ANY}]
   [IPPRotocol={TCP|UDP|ICMp|IGMp|OSPf|NONTcpudp|ANY|
   ip-protocol}]
   [ICmptype={Any|ECHORply|Unreachable|Quench|Redirect|
   ECHO|ADvertisement|Solicitation|TImeexceed|Parameter|
   TSTAMP|TSTAMPRply|INFOREQ|INFOREP|ADDRREQ|ADDRREP|
   NAMEREq|NAMERPly|icmp-type}]
   [ICMPCode={Any|FIlter|FRAGMent|FRAGReassm|HOSTComm|
   HOSTIsolated|HOSTPrec|HOSTREdirect|HOSTRTos|HOSTTos|
   HOSTUNKnown|HOSTUNReach|NETComm|NETREdirect|NETRTos|
   NETTos|NETUNKnown|NETUNReach|NOptr|POrtunreach|
   PREcedent|PROtunreach|PTrproblem|Sourceroute|Ttl|
   icmp-code}]
   [TCPFlags={{Urg|Ack|Rst|Syn|Fin}[,...]|ANY}]
   [TCPDport={port-range|ANY}] [TCPSport={port-range|ANY}]
   [UDPDport={port-range|ANY}] [UDPSport={port-range|ANY}]
```

Description

This command modifies a classifier. Classifiers are packet matching rules that identify particular data flows. The data flows may be specific in nature (e.g. IP packets with a particular TCP destination port from a particular source IP address) or general (e.g. all ICMP packets).

Parameter	Description
CLASSifier	The ID number of the classifier. The ID number determines the rule matching order. Within each traffic class, the classifiers are checked in ascending order of ID number (lowest first). Default: no default
Layer 1 parameters	
EPOrt	The egress port—the Ethernet switch port through which the frame is destined to leave the router. An integer in the range 1 to *n*, where *n* is the highest switch port. Default: **any** (ignores egress port)
IPOrt	The ingress port—the Ethernet switch port through which the frame arrives at the router. An integer in the range 1 to *n*, where *n* is the highest switch port. **Iport** and **iinterface** are mutually exclusive. Default: **any** (ignores ingress port)

Parameter (cont.)	**Description** (cont.)
IINTerface	The ingress interface—the interface through which the frame arrives at the router. Valid entries are Layer 1 and 2 interfaces: ● eth (such as. eth0) ● ATM channel (such as atm0.0) ● frame relay (e.g. fr0) ● PPP (such as ppp0) To see a list of current valid Layer 1 and 2 interfaces, use the **show interface** command in the Interfaces chapter. **Iport** and **iinterface** are mutually exclusive. **Iinterface** is only valid in classifiers for software QoS on egress interfaces or tunnels. Default: **none** (ignores ingress interface)
Layer 2 Ethernet parameters	
SVlan	The source VLAN—the VLAN associated with the frame when it arrives at the router. Only valid in classifiers for software QoS on egress interfaces. Default: **any**
vlan-name	The name of the source VLAN. To see a list of current VLANs, use the **show vlan** command on page 8-54 of Chapter 8, Switching.
1..4094	The VLAN Identifier (VID) of the source VLAN.
ANY	The classifier ignores the source VLAN.
DVlan	The destination VLAN—the VLAN that the frame will be transmitted to. Only valid in classifiers for software QoS on egress interfaces. Default: **any**
vlan-name	The name of the destination VLAN. To see a list of current VLANs, use the **show vlan** command on page 8-54 of Chapter 8, Switching.
1..4094	The VLAN Identifier (VID) of the destination VLAN.
ANY	The classifier ignores the destination VLAN.
VLANPriority	The 802.1p VLAN priority value in the frame. An integer in the range 0 to 7; a range of integers separated by hyphens; or a comma separated list of integers and/or ranges (for example 0,2,4-6). Only valid in classifiers for software QoS on ingress and egress interfaces. Default: **any** (ignores VLAN priority)

Layer 2 Ethernet parameters (cont.)		
ETHFormat	The Ethernet encapsulation type of the frame. The **ethformat** and **protocol** must match. Table 38-1 on page 38-11 shows possible combinations and whether they are valid. You can distinguish between frames that are tagged and untagged at ingress. Default: **any**	
	802.2 802.2-Tagged 802.2-Untagged	Formatted according to IEEE Standards 802.2 and 802.3 with a DSAP/SSAP value not equal to hexadecimal AAAA. Encapsulation: SAP
	Ethii ETHII-Tagged ETHII-Untagged	Formatted according to RFC 894, *Standard for the transmission of IP datagrams over Ethernet networks.* Encapsulation: Ethernet II
	Netwareraw NETWARERAW-Tagged NETWARERAW-Untagged	Formatted as an IPX packet according to IEEE Standard 802.3. Encapsulation: NetWare Raw or Novell
	Snap SNAP-Tagged SNAP-Untagged	Formatted according to IEEE Standards 802.2 and 802.3 and RFC 1042, *Standard for the transmission of IP datagrams over IEEE 802 networks.* Encapsulation: SNAP
	ANY	The classifier ignores the Ethernet encapsulation.
MACDaddr	The destination MAC address of the frame. An Ethernet six-octet MAC address, expressed as six pairs of hexadecimal digits delimited by hyphens. Default: **any** (ignores destination MAC address).	
MACSaddr	The source MAC address of the frame. An Ethernet six-octet MAC address, expressed as six pairs of hexadecimal digits delimited by hyphens. Default: **any** (ignores source MAC address).	
MACType	The type of destination MAC address on the frame. Only valid in classifiers for software QoS on egress interfaces. Default: **any**	
	L2Ucast	Layer 2 unicast addresses.
	L2BMcast	Layer 2 broadcast or multicast addresses.
	ANY	The classifier ignores the MAC address type.

Layer 2 Ethernet parameters (cont.)

PROTocol — The protocol, determined from the value of the following Ethernet field:

- for 802.2 (SAP encapsulation): the DSAP field, 1 byte hexadecimal
- for ETHII encapsulation: the ETYPE field, 2 bytes hexadecimal
- for NETWARERAW encapsulation: the IPX checksum field, 2 bytes hexadecimal with value FFFF
- for SNAP encapsulation: the ETYPE field, 5 bytes hexadecimal. The classifier matches on the last 2 bytes.

The encapsulation type (**ethformat** parameter) and **protocol** must match. Table 38-1 on page 38-11 shows possible combinations and whether they are valid.

Default: **any**, unless you also specify a TCP or UDP parameter (for example, **tcpsport**). Then the default is **IP**.

protocol-type	The protocol number or the predefined protocol name. Table 38-2 on page 38-13 shows predefined protocols, their numbers, and their encapsulations.
IP	Internet Protocol version 4. Valid with **ethformat** of **ethii** or **snap**.
IPV6	Internet Protocol version 6. Valid with **ethformat** of **ethii**.
ARP	Address Resolution Protocol. Valid with **ethformat** of **ethii** or **snap**.
IPX	IPX. Valid with **ethformat** of **802.2**, **ethii**, **netwareraw** or **snap**.
ANY	The classifier ignores the protocol.

Layer 2 parameters (ATM, frame relay and PPP)

ATMVCi — The Virtual Channel Identifier for an ATM connection. An integer in the range 0 to 255, or a range of integers separated by a hyphen (for example 0-3). Only valid in classifiers for software QoS on egress interfaces.

Default: **any** (ignores ATM VCI).

ATMVPi — The Virtual Path Identifier for an ATM connection. An integer in the range 0 to 4095, or a range of integers separated by a hyphen (for example 0-3). Only valid in classifiers for software QoS on egress interfaces.

Default: **any** (ignores ATM VPI).

DLCi — The identification number of a Frame Relay Data Link Connection (DLC). An integer in the range 0 to 1023, or a range of integers separated by a hyphen (for example 0-3). Only valid in classifiers for software QoS on egress interfaces.

Default: **any** (ignores DLCI).

PPPIndex — The PPP interface number. For example, for ppp2, **pppindex**=**2**.

Layer 2 parameters (ATM, frame relay and PPP) (cont.)		
PPPProtocolid	The network layer protocol of the PPP encapsulated packet. Note that network and link control packets are processed by the software QoS policy's system traffic class. Examples of control packets include NCP, LCP, IPCP and PAP. Only valid in classifiers for software QoS on egress interfaces. Default: **any**, unless you also specify a TCP or UDP parameter. Then the default is **IP**.	
	ppp-protocol-id|	A 4 byte hexadecimal protocol number. Table 38-3 on page 38-14 shows valid protocols and numbers.
	IP	Internet Protocol.
	IPV6	Internet Protocol version 6.
	ANY	The classifier ignores PPP protocol ID.
Layer 3 parameters		
IPDAddr	The destination IPv4 or IPv6 address of the packet. Default: **any**	
	ipadd[/0..32]	The destination IPv4 address, in dotted decimal notation. You can optionally specify a subnet by specifying a mask.
	ipv6add[/0..128]	The destination IPv6 address, specified as eight pairs of hexadecimal octets separated by colons. You can optionally specify a prefix length. Default prefix length is 128—a single address. IPv6 addresses are only valid in classifiers for software QoS on egress or tunnel interfaces.
	ANY	The classifier ignores destination IP or IPv6 address.
IPSAddr	The source IPv4 or IPv6 address of the packet. Default: **any**	
	ipadd[/0..32]	The source IPv4 address, in dotted decimal notation. You can optionally specify a subnet by specifying a mask.
	ipv6add[/0..128]	The source IPv6 address, specified as eight pairs of hexadecimal octets separated by colons. You can optionally specify a prefix length. Default prefix length is 128—a single address. IPv6 addresses are only valid in classifiers for software QoS on egress or tunnel interfaces.
	ANY	The classifier ignores source IPv4 or IPv6 address.
IPDScp	The DSCP value—the Code Point bits of the DiffServ field of an IPv4 or IPv6 packet. An integer in the range 0 to 63; a range of integers separated by hyphens; or a comma separated list of integers and/or ranges (for example 0,2,4-6). You can also specify EF, AF1, AF2, AF3 or AF4. **Ipdscp** and **Iptos** are mutually exclusive. Default: **any** (ignores DSCP).	
IPTOs	The TOS value—the value of the precedence field within the TOS byte of an IPv4 packet. An integer in the range 0 to 7. **Ipdscp** and **Iptos** are mutually exclusive. **Iptos** is only valid for IPv4 packets. Default: **any** (ignores TOS).	

Layer 3 parameters (cont.)	
IPFRAg	Whether the IPv4 packet is fragmented. Only valid in classifiers for software QoS on egress or tunnel interfaces. Default: **any** (ignores whether the packet is fragmented).
IPOPtions	Whether the packet includes the IPv4 header options field. Only valid in classifiers for software QoS on egress or tunnel interfaces. Default: **any** (ignores whether the header options field is present or not).
IPFLowlabel	The IPv6 flow label in an IPv6 packet, an integer in the range 0 to 1048575. Only valid for IPv6 packets in classifiers for software QoS on egress or tunnel interfaces. Default: **any** (ignores IPv6 flow label).
IPPRotocol	The Layer 4 IPv4 or IPv6 protocol of the packet. For IPv6 packets, **ipprotocol** matches against the Next Header field of the IPv6 packet header. You can use a total of 29 unique **ipprotocol** values, plus TCP and UDP, in total across all classifiers. Default: ● **tcp** if you also specify a TCP parameter (for example, **tcpsport**). ● **udp** if you also specify a UDP parameter (for example, **udpsport**). ● Otherwise, **any** (ignores IP protocol).

ip-protocol	A 1 byte decimal IPv4 or IPv6 protocol number or a well-known protocol name.
TCP	Transmission Control Protocol.
UDP	User Datagram Protocol.
NONTcpudp	Any IPv4 or IPv6 protocol except TCP or UDP.
ICMp	Internet Control Message Protocol.
IGMp	Internet Group Multicast Protocol.
OSPf	Open Shortest Path First.
ANY	The classifier ignores the IP protocol value.

Layer 4 parameters	
ICmptype	The ICMP message type to match against the ICMP type field in an ICMP packet header. One of the list of options, or a decimal value in the range 0 to 65535. Only valid if **ipprotocol=icmp** in classifiers for software QoS on egress or tunnel interfaces. Default: **any** (ignores ICMP type).
ICMPCode	The ICMP message reason code to match against the ICMP code field in an ICMP packet header. One of the list of options, or a decimal value in the range 0 to 65535. Only valid if **ipprotocol=icmp** in classifiers for software QoS on egress or tunnel interfaces. Default: **any** (ignores ICMP code).
TCPFlags	The TCP flags of the TCP/IP packet. One or a comma-separated list of the options URG, ACK, RST, SYN and FIN. Default: **any** (ignores TCP flag).
TCPDport	The destination TCP port—the value in the TCP destination port field of the packet. For classifiers for software QoS on egress or tunnel interfaces, a single port number or a range of port numbers separated by a hyphen. Default: **any** (ignores destination TCP port).

Layer 4 parameters (cont.)	
TCPSport	The source TCP port—the value in the TCP source port field of the packet. For classifiers for software QoS on egress or tunnel interfaces, a single port number or a range of port numbers separated by a hyphen. Default: **any** (ignores source TCP port).
UDPDport	The destination UDP port—the value in the UDP destination port field of the packet.For classifiers for software QoS on egress or tunnel interfaces, a single port number or a range of port numbers separated by a hyphen. Default: **any** (ignores destination UDP port).
UDPSport	The source UDP port—the value in the UDP source port field of the packet. For classifiers for software QoS on egress or tunnel interfaces, a single port number or a range of port numbers separated by a hyphen. Default: **any** (ignores source UDP port).

Examples

To set packet matching rule 1 so that it matches all IP packets from the IP subnet 192.168.100.2 (mask=255.255.255.0), with a destination TCP port of 23, use one of the commands:

```
set class=1 ipsa=192.168.100.2/24 tcpd=23
set class=1 prot=ip ipsa=192.168.100.2/24 tcpd=23
```

To change packet matching rule 2 so that it matches traffic over ppp3, use the command:

```
set class=2 pppi=3
```

Related Commands

create classifier
destroy classifier
show classifier

show classifier

Syntax `SHow CLASSifier[={`*`id-list`*`|ALL|DYnamic}]`

Description This command displays information about the classifiers configured.

If you specify **classifier** with no value, then a summary of all classifiers is displayed (Figure 38-1 and Table 38-4).

If you specify **classifier**=**all**, then details of all classifiers are displayed.

If you specify **classifier**=*id-list*, then details of the specified classifiers are displayed.

If you specify **classifier**=**dynamic**, then details of classifiers created by the DAR objects are displayed.

Figure 38-1: Example summary output from the **show classifier** command

```
 Classifier General Info
-------------------------------------------------------------
 Total number of rules .... 6

 Rule  Type            Related Module(s)
---------------------------------------
 1     L2              L3 switch
 2     L2              L3 switch, QOS
 100   L4,L3,L2        QOS, Software QoS
 200   L3,L2           L3 switch, QOS, Software QoS
 700   L3              None
 9999  Match all       None
-------------------------------------------------------------
```

Table 38-4: Parameters in the summary output of the **show classifier** command

Parameter	Meaning
Rule	The identifier number for the classifier.
Type	A list of OSI layers at which parameters with non-default values in the rule operate, items in the list include L5, L4, L3, L2 and L1.
Related module(s)	The name of the module(s) that are currently using the classifier.

Figure 38-2: Example summary output from the **show classifier=all** command

```
 Classifier Rules
-------------------------------------------------------------
 Rule .................. 1
  VLAN ................. default (1)

 Rule .................. 2
  VLAN ................. v2 (2)

 Rule .................. 100
  Protocol ............. IP
  D-IP Address ......... 10.0.0.1/32
  IP Protocol .......... TCP
  D-TCP Port ........... 23

 Rule .................. 200
  Protocol ............. IP
  D-IP Address ......... 10.0.0.1/32

 Rule .................. 700
  MATCH1 ............... 1111
  MASK1 ................ 2222
  OFFSET1 .............. 1

 Rule .................. 9999
  Match all frames
-------------------------------------------------------------
```

Table 38-5: Parameters in the summary output of the **show classifier= all** command

Parameter	Meaning
Rule	The identifier number for the classifier.
VLAN	The name of a VLAN with only the first 10 characters shown. The VLAN Identifier appears in brackets. If the packet is Layer 3 switched, this VLAN is the destination VLAN. If the packet is Layer 3 routed by the CPU, this VLAN is the source VLAN. If the packet is Layer 2 switched, its source and destination VLAN are the same.
Protocol	The hexadecimal value of the protocol. If the protocol is not for the general family of IP and IPX protocols, and the commonly known name for the protocol is known to the Classifier, then this commonly known name will be printed in brackets after the hexadecimal number.
D-IP Address	The destination IP address field of a packet.
IP Protocol	The Layer 4 IP protocol field of a packet.
D-TCP Port	The destination TCP/IP port field of a packet.
MATCH1	A 16-bit word to match inside a packet.
MASK1	A 16-bit word used as a mask for the MATCH1 parameter value.
OFFSET1	The offset from the start of the packet.

Figure 38-3: Example detailed output from the **show classifier=2,3** command for classifiers that can be applied to software QoS

```
 Classifier Rules
-----------------------------------------------------------------
 Rule .................. 2
  Ingress Port ......... 1

 Rule .................. 3
  Protocol ............. IP
  DSCP ................. 10,12,14 (AF1)
-----------------------------------------------------------------
```

Figure 38-4: Example output from the **show classifier=dynamic** command

```
 Classifier Rules
-----------------------------------------------------------------
 Rule .................. 10001
  Protocol ............. IPv4/IPv6
  IP Protocol .......... UDP
  D-UDP Port ........... 42768
-----------------------------------------------------------------
```

Table 38-6: Parameters in the detailed output of the **show classifier** command for classifiers that can be applied to software QoS

Parameter	Meaning
Rule	The ID number of the classifier. The software QoS traffic class ID number and classifier ID number together determine the rule matching order. Classifiers within each traffic class are checked in ascending order of ID number (lowest first).
Egress Port	The Ethernet switch port through which the frame is destined to leave the router.
Ingress Port	The Ethernet switch port through which the frame arrives at the router.
Ingress Interface	The interface through which the frame arrives at the router.
D-MAC Address	The destination MAC address of the frame.
S-MAC Address	The source MAC address of the frame.
M-Type	The type of destination MAC address on the frame; one of L2Ucast (Layer 2 unicast addresses), L2Mcast (Layer 2 multicast addresses), L2Bcast (Layer 2 broadcast addresses) L2BMcast (Layer 2 broadcast or multicast addresses) or ANY.
S-VLAN	The source VLAN—the VLAN associated with the frame when it arrives at the router.
D-VLAN	The destination VLAN—the VLAN that the frame will be transmitted to.
E-Format	The Ethernet encapsulation type of the frame.
Protocol	The protocol, determined from the value of the following Ethernet field: ● for 802.2 (SAP encapsulation): the DSAP field, 1 byte hexadecimal ● for ETHII encapsulation: the ETYPE field, 2 bytes hexadecimal ● for NETWARERAW encapsulation: the IPX checksum field, 2 bytes hexadecimal with value FFFF ● for SNAP encapsulation: the ETYPE field, 5 bytes hexadecimal. The classifier matches on the last 2 bytes.
VLAN Priority	The 802.1p VLAN priority value in the frame.
ATM VCI	The Virtual Channel Identifier for an ATM connection.
ATM VPI	The Virtual Path Identifier for an ATM connection.
DLCI	The identification number of a Frame Relay Data Link Connection (DLC).
PPP Index	The PPP interface number. For example, for ppp2, PPP Index is 2.
PPP Protocol ID	The network layer protocol of the PPP encapsulated packet. Table 38-3 on page 38-14 shows valid protocols and numbers. Note that network and link control packets are processed by the software QoS policy's system traffic class. Examples of control packets include NCP, LCP, IPCP and PAP.
S-IP Address	The source IPv4 or IPv6 address of the packet.
D-IP Address	The destination IPv4 or IPv6 address of the packet.
IP flow label	The IPv6 flow label in an IPv6 packet.
IP Protocol	The Layer 4 IPv4 or IPv6 protocol of the packet. For IPv6 packets, IP protocol matches against the Next Header field of the IPv6 packet header.

Table 38-6: Parameters in the detailed output of the **show classifier** command for classifiers that can be applied to software QoS (cont.)

Parameter	Meaning
DSCP	The DSCP value—the Code Point bits of the DiffServ field of an IPv4 or IPv6 packet.
TOS	The TOS value—the value of the precedence field within the TOS byte of an IPv4 packet.
IPOPTIONS	Whether the packet includes the IPv4 header options field.
IPFRAG	Whether the IPv4 packet is fragmented.
ICMP Code	The ICMP message reason code to match against the ICMP code field in an ICMP packet header.
ICMP Type	The ICMP message type to match against the ICMP type field in an ICMP packet header.
S-TCP Port	The source TCP port—the value in the TCP source port field of the packet.
D-TCP Port	The destination TCP port—the value in the TCP destination port field of the packet.
TCP Flags	The TCP flags of the TCP/IP packet. One or a comma-separated list of the options URG, ACK, RST, SYN and FIN.
S-UDP Port	The source UDP port—the value in the UDP source port field of the packet.
D-UDP Port	The destination UDP port—the value in the UDP destination port field of the packet.

Examples

To display the number of each of the classifiers and which module is using each classifier, use the command:

```
sh class
```

To display what each classifier matches against, use the command:

```
sh class=all
```

Related Commands

create classifier
destroy classifier
set classifier